# ESET ENDPOINT SECURITY

## Guia do Usuário

Microsoft® Windows® 8 / 7 / Vista / XP / 2000 / Home Server

Clique aqui para fazer download da versão mais recente deste documento

eset

# ESET ENDPOINT SECURITY



Atendimento ao cliente mundial www.eset.com/support

REV. 20. 2. 2013

# Índice

# 1. ESET Endpoint Security

ESET Endpoint Security representa uma nova abordagem para a segurança do computador verdadeiramente integrada. A versão mais recente do mecanismo de rastreamento ThreatSense®, combinada com o firewall pessoal personalizado e o módulo antispam, utiliza velocidade e precisão para manter o computador seguro. O resultado é um sistema inteligente que está constantemente em alerta contra ataques e programas maliciosos que podem comprometer o funcionamento do computador.

ESET Endpoint Security é uma solução de segurança completa desenvolvida a partir do nosso esforço de longo prazo para combinar proteção máxima e impacto mínimo no sistema. As tecnologias avançadas, com base em inteligência artificial, são capazes de eliminar proativamente a infiltração por vírus, spywares, cavalos de troia, worms, adwares, rootkits e outros ataques via Internet sem prejudicar o desempenho do sistema ou interromper a atividade do computador.

O ESET Endpoint Security foi projetado principalmente para o uso em estações de trabalho em um ambiente de negócios/empresarial. É possível usá-lo com o ESET Remote Administrator, permitindo gerenciar facilmente qualquer número de estações de trabalho do cliente, aplicar políticas e regras, monitorar detecções e configurar remotamente a partir de qualquer computador em rede.

## 1.1 Requisitos do sistema

Para uma operação sem interrupções do ESET Endpoint Security, o sistema deve atender aos seguintes requisitos de hardware e de software:

**Microsoft® Windows® 2000, XP**

400 MHz 32 bits (x86)/64 bits (x64)
128 MB de memória RAM do sistema
320 MB de espaço disponível
Super VGA (800 x 600)

**Microsoft® Windows® 8, 7, Vista, Home Server**

1 GHz 32 bits (x86)/64 bits (x64)
512 MB de memória RAM do sistema
320 MB de espaço disponível
Super VGA (800 x 600)

## 1.2 Prevenção

Quando você trabalhar com o computador, e especialmente quando navegar na Internet, tenha sempre em mente que nenhum sistema antivírus do mundo pode eliminar completamente o risco causado pelas ameaças e ataques. Para fornecer proteção e conveniência máximas, é essencial usar o sistema antivírus corretamente e aderir a diversas regras úteis.

**Atualização regular**

De acordo com as estatísticas do ESET Live Grid, milhares de novas ameaças únicas são criadas todos os dias a fim de contornar as medidas de segurança existentes e gerar lucro para os seus autores - todas às custas dos demais usuários. Os especialistas no Laboratório de vírus da ESET analisam essas ameaças diariamente, preparam e publicam atualizações a fim de melhorar continuamente o nível de proteção dos usuários do programa antivírus. Uma atualização configurada incorretamente diminui a eficiência do programa. Para obter mais informações sobre como configurar as atualizações, consulte o capítulo Configuração da atualização.

**Download dos patches de segurança**

Os autores dos softwares maliciosos preferem explorar as diversas vulnerabilidades do sistema a fim de aumentar a eficiência da disseminação do código malicioso. Essa é a razão pela qual as empresas de software vigiam de perto as novas vulnerabilidades em seus aplicativos para elaborar e publicar atualizações de segurança, eliminando as ameaças em potencial regularmente. É importante fazer o download dessas atualizações de segurança à medida que são publicadas. Os exemplos de tais aplicativos incluem o sistema operacional Windows ou o navegador da internet amplamente usado, o Internet Explorer.

### Backup dos dados importantes

Os escritores dos softwares maliciosos não se importam com as necessidades dos usuários, e a atividade dos programas maliciosos frequentemente leva ao mau funcionamento de um sistema operacional e a danos deliberados dos dados importantes. É importante fazer o backup regular dos seus dados importantes e sensíveis para uma fonte externa como um DVD ou disco rígido externo. Precauções como essas tornam mais fácil e rápido recuperar os seus dados no caso de falha do sistema.

### Rastreie regularmente o seu computador em busca de vírus

Um rastreamento automático regular do computador com as configurações corretas pode remover as ameaças que podem ter escapado às atualizações de assinaturas de vírus antigas.

### Siga as regras básicas de segurança

Essa é a regra mais útil e eficiente de todas - seja sempre cauteloso. Hoje, muitas ameaças exigem a interação do usuário para serem executadas e distribuídas. Se você for cauteloso ao abrir novos arquivos, economizará tempo e esforço consideráveis que, de outra forma, seriam gastos limpando as ameaças do seu computador. Algumas regras úteis:

- Não visite sites suspeitos com inúmeras pop-ups e anúncios piscando.
- Seja cuidadoso ao instalar programas freeware, pacotes codec. etc. Use somente programas seguros e somente visite sites da Internet seguros.
- Seja cauteloso ao abrir anexos de e-mail, especialmente aqueles de mensagens spam e mensagens de remetentes desconhecidos.
- Não use a conta do Administrador para o trabalho diário em seu computador.

## 2. Instalação

Inicie o instalador e o assistente de instalação o guiará pelo processo de configuração.

**Importante:** Verifique se não há algum outro programa antivírus instalado no computador. Se duas ou mais soluções antivírus estiverem instaladas em um único computador, elas podem entrar em conflito umas com as outras. Recomendamos desinstalar outros programas antivírus do sistema. Consulte nosso artigo da base de conhecimento para obter uma lista de ferramentas de desinstalação para os softwares de antivírus comuns (disponível em inglês e vários outros idiomas).

Configuração do ESET Endpoint Security

ESET ENDPOINT SECURITY RC

**Bem vindo ao Assistente de instalação do ESET Endpoint Security**

O Assistente de instalação vai instalar o ESET Endpoint Security no seu computador. Clique em Próximo para continuar ou Cancelar para sair do Assistente de instalação.

**Aviso!**

Antes de continuar a instalação e para evitar graves problemas, desinstale imediatamente qualquer outro aplicativo de segurança residente, como programas antivírus, antispyware ou firewall, que possam estar sendo executados.

< Anterior | Próximo > | Cancelar

Primeiro, o programa verifica se há uma versão mais nova do ESET Endpoint Security disponível. Se uma versão mais recente for encontrada, você será notificado na primeira etapa do processo de instalação. Se selecionar a opção **Fazer download e instalar nova versão**, a nova versão será obtida por download e a instalação continuará. Na próxima etapa, o Contrato de licença de usuário final será exibido. Leia-o e clique em **Aceitar** para confirmar a sua aceitação do Contrato de licença de usuário final. Após aceitar, a instalação continuará em dois cenários possíveis:

1. Se estiver instalando o ESET Endpoint Security em um computador pela primeira vez, você verá a janela a seguir após aceitar o **Contrato de licença de usuário final**. Aqui, você pode escolher entre uma Instalação típica e uma Instalação personalizada e continuar.

Configuração do ESET Endpoint Security

**Modo de instalação**

Seleção do modo de instalação

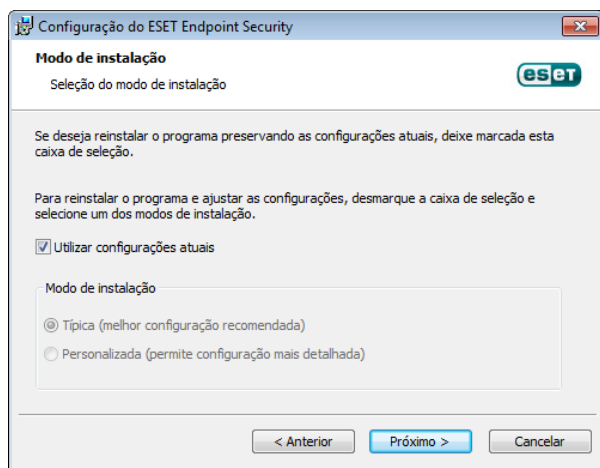
Por favor, escolha se deseja instalar o ESET Endpoint Security com configurações Típicas (fornece o melhor equilíbrio entre segurança e velocidade) ou Personalizada para obter opções de configurações adicionais.

Modo de instalação

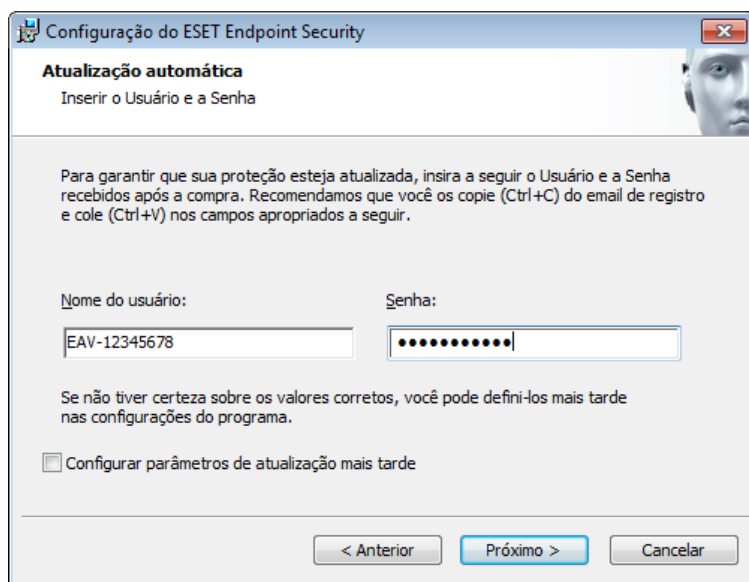
Típica (melhor configuração recomendada)

Personalizada (permite configuração mais detalhada)

< Anterior | Próximo > | Cancelar

2. Se você estiver instalando o ESET Endpoint Security sobre uma versão anterior desse software, a seguinte janela permitirá que você escolha usar as configurações atuais do programa para a nova instalação, ou, se a opção **Utilizar configurações atuais** for desmarcada, escolha entre os dois modos de instalação mencionados anteriormente.

## 2.1 Instalação típica

O modo de instalação Típica inclui as opções de configuração apropriadas para a maioria dos usuários. Essas configurações proporcionam excelente segurança, configuração fácil e alto desempenho do sistema. A instalação típica é a opção padrão e é recomendada se você não tiver requisitos particulares para configurações específicas.

Após selecionar o modo de instalação e clicar em **Avançar**, você será solicitado a inserir o nome de usuário e a senha. Essa etapa tem um papel significativo no fornecimento de proteção constante ao seu sistema.

Insira o seu **Nome de usuário** e **Senha**, isto é, os dados de autenticação recebidos após a compra ou registro do produto, nos campos correspondentes. Caso você não tenha o nome de usuário e a senha disponíveis no momento, clique na caixa de seleção **Configurar parâmetros de atualização mais tarde**. O nome de usuário e senha podem ser inseridos no programa posteriormente.

A próxima etapa é a configuração do ESET Live Grid. O ESET Live Grid ajuda a assegurar que a ESET seja informada contínua e imediatamente sobre novas infiltrações para proteger seus clientes. O sistema permite o envio de novas ameaças para o Laboratório de vírus da ESET, onde elas são analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus.

Configuração do ESET Endpoint Security

**ESET Live Grid**

Criado a partir do sistema de alerta antecipado avançado ThreatSense.net, o ESET Live Grid foi projetado para fornecer níveis adicionais de segurança ao seu computador. Ele monitora constantemente os programas em execução no sistema e processa com relação à inteligência mais recente coletada de milhões de usuários do ESET em todo o mundo. Adicionalmente, os rastreamentos do sistema são processados mais rapida e precisamente à medida que o banco de dados do ESET Live Grid cresce no decorrer do tempo.

Eu concordo em participar do ESET Live Grid (recomendado)

< Anterior | Próximo > | Cancelar

Por padrão, a opção **Concordo em participar do ESET Live Grid** está selecionada, o que ativará este recurso.

A próxima etapa do processo de instalação é a configuração da detecção de aplicativos potencialmente não desejados. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Consulte o capítulo Aplicativos potencialmente indesejados para obter mais detalhes.

Configuração do ESET Endpoint Security

**Detecção de aplicativos potencialmente não desejados**

Aplicativos potencialmente não desejados são programas que normalmente requerem o consentimento do usuário antes da instalação. Eles podem não oferecer riscos diretos de segurança, mas podem afetar o desempenho, a velocidade, a confiabilidade e o comportamento de seu computador.

Selecione uma das opções
Selecione uma das opções
Ativar detecção de aplicativos potencialmente não desejados
Desativar detecção de aplicativos potencialmente não desejados

< Anterior | Próximo > | Cancelar

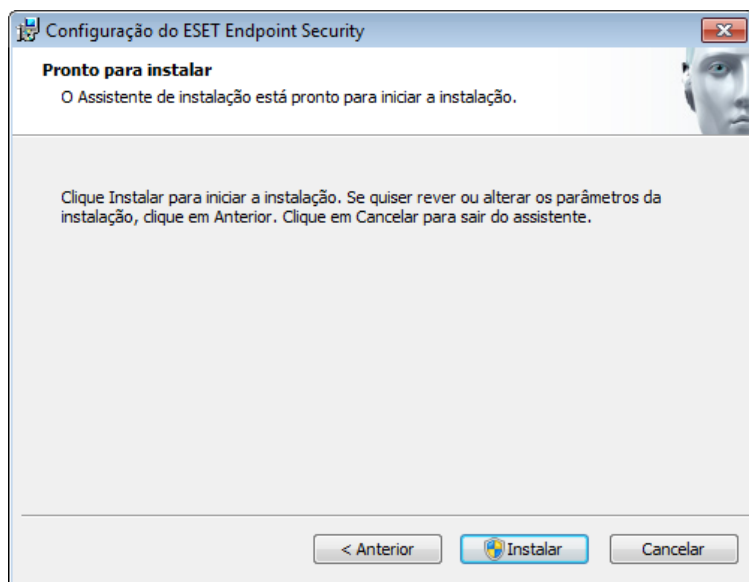
A última etapa no modo de instalação Típica é confirmar a instalação clicando no botão **Instalar**.

Configuração do ESET Endpoint Security

**Pronto para instalar**

O Assistente de instalação está pronto para iniciar a instalação.

Clique Instalar para iniciar a instalação. Se quiser rever ou alterar os parâmetros da instalação, clique em Anterior. Clique em Cancelar para sair do assistente.

< Anterior | Instalar | Cancelar

## 2.2 Instalação personalizada

O modo de instalação personalizada é destinado a usuários experientes e que desejam modificar configurações avançadas durante a instalação.

Após selecionar este modo de instalação e clicar em **Avançar**, será preciso definir um local de destino para a instalação. Por padrão, o programa é instalado no seguinte diretório:

C:\Program Files\ESET\ESET Endpoint Security\

Clique em **Procurar...** para alterar o local (não recomendado).

Configuração do ESET Endpoint Security

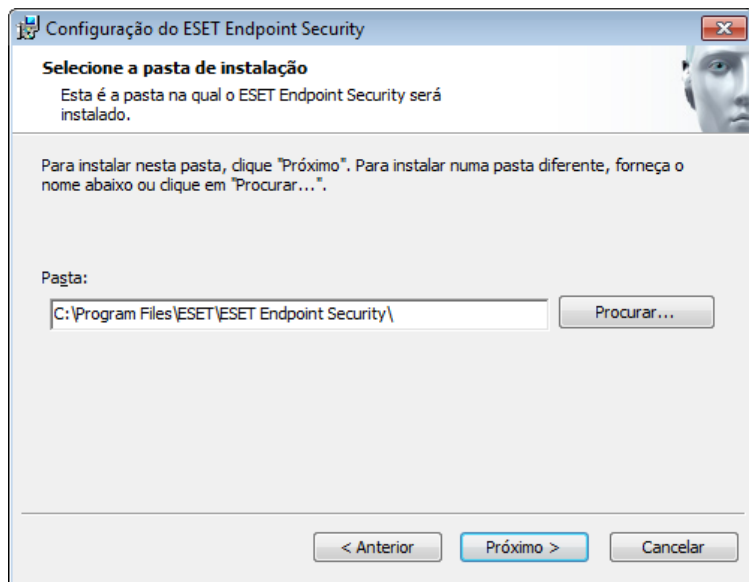
**Selecione a pasta de instalação**

Esta é a pasta na qual o ESET Endpoint Security será instalado.

Para instalar nesta pasta, clique "Próximo". Para instalar numa pasta diferente, forneça o nome abaixo ou clique em "Procurar...".

Pasta:

C:\Program Files\ESET\ESET Endpoint Security\ | Procurar...

< Anterior | Próximo > | Cancelar

Em seguida, insira o **Nome de usuário** e a **Senha**. Essa etapa é igual à da instalação Típica (consulte "Instalação típica").

A próxima etapa do processo de instalação é selecionar os componentes do programa a serem instalados. Ao expandir a árvore de componentes e selecionar um recurso, as opções de instalação da árvore serão exibidas. A opção **Serão instaladas para serem executadas a partir do disco local** está selecionada por padrão. Ao selecionar **Todas as funcionalidades serão instaladas para serem executadas a partir do disco local** instalará todos os recursos na árvore selecionada. Se não deseja usar um recurso ou um componente, selecione **Todas as funcionalidades não estarão disponíveis**.

Configuração do ESET Endpoint Security

**Seleção dos componentes do programa**

Selecione os componentes do programa a instalar

- Computador
- Rede
- Web e email
  - Filtragem de protocolo
  - Proteção do cliente de email

Serão instaladas para serem executadas a partir disco local

Todas as funcionalidades serão instaladas para serem executadas a partir do disco local

Todas as funcionalidades não estarão disponíveis

A proteção do cliente de email rastreia o tráfego de entrada e saída de emails no seu computador. Suporta os seguintes clientes de email: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.

< Anterior | Próximo > | Cancelar

Clique em **Avançar** e continue para configurar a conexão com a Internet. Se você usa um servidor proxy, ele deve ser configurado corretamente para que as atualizações das assinaturas de vírus funcionem. Se não tiver certeza se utiliza ou não um servidor proxy para conectar-se à Internet, selecione **Não tenho a certeza se a minha conexão com a Internet utiliza um servidor proxy. Use as mesmas configurações usadas pelo Internet Explorer (Recomendável)** e clique em **Avançar**. Se você não utilizar um servidor proxy, selecione a opção **Eu não utilizo um servidor proxy**.

Configuração do ESET Endpoint Security

**Conexão com a Internet**

Configurar sua conexão com a Internet

Selecione as opções correspondentes ao seu tipo de conexão à Internet. Se você não tiver certeza, selecione as configurações utilizadas pelo Internet Explorer.

Servidor proxy

- Não tenho a certeza se minha conexão com a Internet utiliza um servidor proxy. Utilize as mesmas configurações do Internet Explorer. (Recomendável)
- Eu não utilizo um servidor proxy
- Eu utilizo um servidor proxy

< Anterior | Próximo > | Cancelar

Para definir as configurações do servidor proxy, selecione **Eu utilizo um servidor proxy** e clique em **Avançar**. Digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Caso o servidor proxy exija autenticação, digite um **usuário** e uma **senha** válidos a fim de obter acesso ao servidor proxy. As configurações do servidor proxy também podem ser copiadas do Internet Explorer se desejar. Para fazer isso, clique em **Aplicar** e confirme a seleção.

Configuração do ESET Endpoint Security

**Servidor proxy**

Inserir parâmetros de servidor proxy

Configurações do servidor proxy:

Endereço: 192.168.1.1

Porta: 3128

Nome do usuário: user

Senha: •••••••••

Utilizar configurações do Internet Explorer

Endereço:

Porta:

Aplicar

< Anterior | Próximo > | Cancelar

Essa etapa de instalação permite designar como as atualizações automáticas do programa serão tratadas no sistema. Clique em **Alterar...** para acessar as configurações avançadas.

Configuração do ESET Endpoint Security

**Atualização automática**

Configurar definições de atualização automática

O Assistente de instalação agora agendará as tarefas que irão garantir as atualizações automáticas do programa. Você pode editar as tarefas de atualização conforme suas necessidades, usando o Agendador a qualquer momento.

Tipo de atualização

Componentes do programa: Sugerir [Alterar...]

[< Anterior] [Próximo >] [Cancelar]

Se não desejar atualizar os componentes do programa, selecione **Nunca atualizar componentes de programa**. Selecione a opção **Perguntar antes de fazer download dos componentes de programa** para exibir uma janela de confirmação sempre que o sistema tentar fazer download dos componentes de programa. Para fazer download automaticamente de atualizações dos componentes do programa, selecione a opção **Sempre atualizar componentes do programa**.

Configuração do ESET Endpoint Security

Atualizações podem ser realizadas automaticamente sem a interferência do usuário, ou você pode se notificado antes do início da atualização. Após a atualização de componentes do programa, a reinicialização pode ser requerida.

Atualização de componente de programa

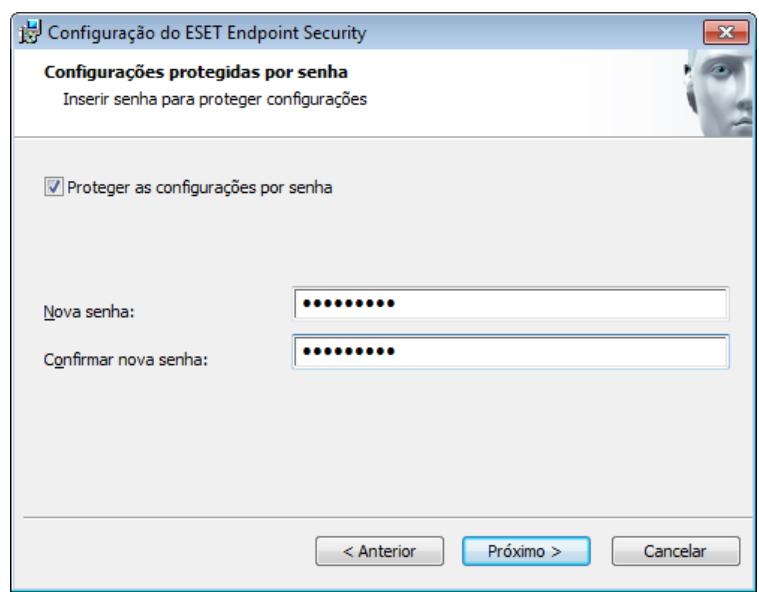
- Nunca atualizar componentes de programa
- Sempre atualizar componentes do programa
- Perguntar antes de atualizar os componentes do programa

Reiniciar depois da atualização do componente de programa

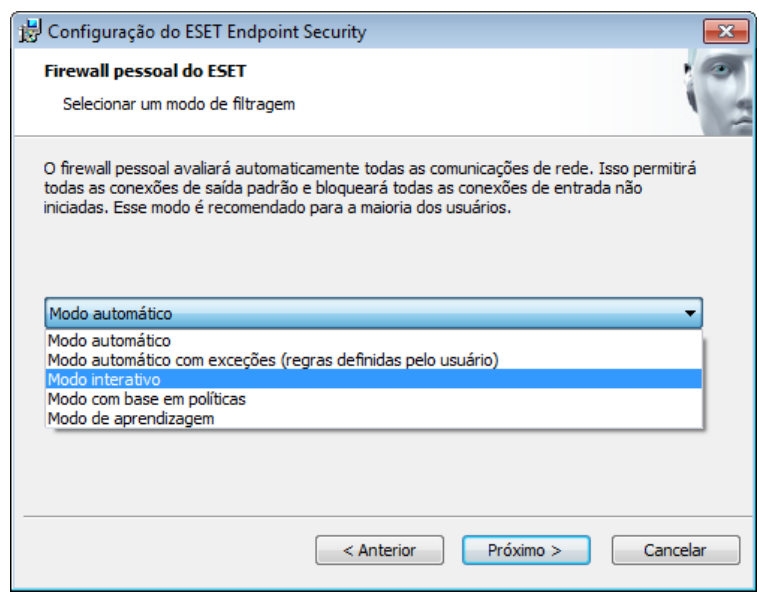
- Nunca reiniciar o computador
- Sugerir opção de reinicialização do computador, se necessário
- Se necessário, reinicialize o computador sem notificação

[OK] [Cancelar]

**OBSERVAÇÃO:** Após a atualização dos componentes do programa, geralmente é necessária a reinicialização do sistema. Recomendamos selecionar a opção **Se necessário, reiniciar o computador sem notificar**.

A próxima janela da instalação oferecerá a opção de definir uma senha para proteger as configurações do programa. Selecione a opção **Proteger as configurações por senha** e digite a sua senha nos campos **Nova senha** e **Confirmar nova senha**. Esta senha será solicitada em todas modificações ou acessos futuros no ESET Endpoint Security. Quando ambos os campos de senha coincidirem, clique em **Avançar** para continuar.



As próximas etapas da instalação, a **Atualização automática**, o **ESET Live Grid** e a **Detecção de aplicativos potencialmente não desejados** serão tratadas da mesma forma que no modo Instalação típica (consulte "Instalação típica").

Em seguida, selecione um modo de filtragem para o firewall pessoal da ESET. Cinco modos de filtragem estão disponíveis para o firewall pessoal do ESET Endpoint Security. O comportamento do firewall é alterado com base no modo selecionado. Os Modos de filtragem também influenciam o nível de interação necessário do usuário.



Clique em **Instalar** na janela **Pronto para instalar** para concluir a instalação. Após a conclusão da instalação, você será solicitado a ativar o produto. Consulte Instalação típica para obter mais informações sobre a ativação do produto.

## 2.3 Inserção do usuário e da senha

Para obter a funcionalidade ideal, é importante que o programa seja atualizado automaticamente. Isso somente será possível se o nome de usuário e a senha corretos forem digitados na **Configuração de atualização**.

Se você não inseriu o seu nome de usuário e senha durante a instalação, poderá inseri-los agora. Pressione **CTRL+U** e insira os dados recebidos com a licença do produto de segurança ESET na janela Detalhes da licença.

Ao inserir seu **Nome de usuário** e **Senha**, é importante digitá-los exatamente como foram gravados:

- O nome de usuário e a senha fazem diferenciação de maiúsculas, minúsculas e hífens, se necessário.
- A senha tem dez caracteres e todos minúsculos.
- Não usamos a letra L em senhas (use o número um (1) no lugar da letra).
- Um 'O' mais alto é o número zero (0), um 'o' mais baixo é a letra 'o' minúscula.

Recomendamos que você copie e cole os dados do email de registro para garantir a precisão.

## 2.4 Atualização para uma versão mais recente

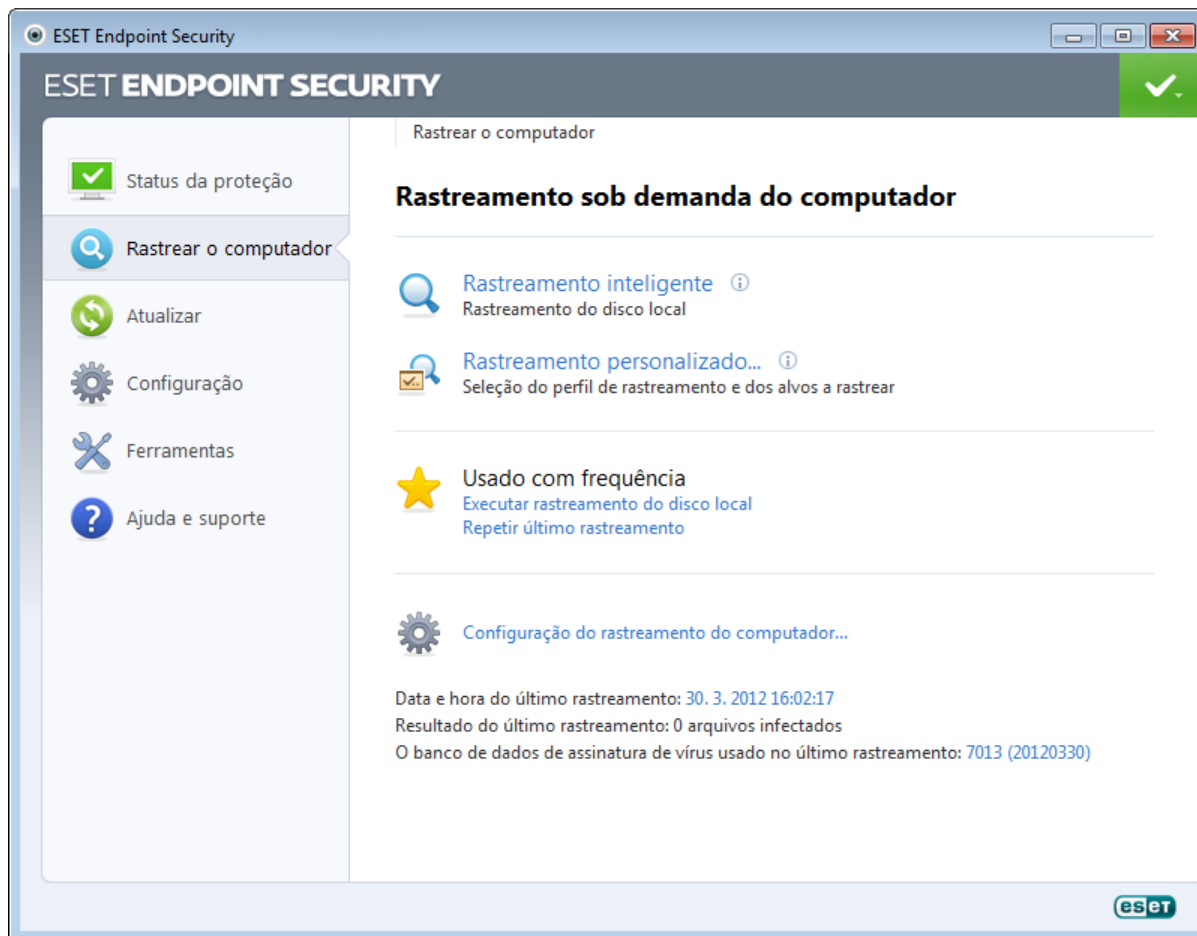
Versões mais recentes do ESET Endpoint Security são lançadas para trazer aprimoramentos ou corrigir problemas que não podem ser resolvidos por meio de atualizações automáticas dos módulos do programa. A atualização para uma versão mais recente pode ser feita de várias formas:

1. Automaticamente, por meio de uma atualização do programa
   Como a atualização do programa é distribuída para todos os usuários e pode ter impacto em determinadas configurações do sistema, ela é lançada depois de um longo período de testes para funcionar com todas as configurações de sistema possíveis. Se você precisar atualizar para uma versão mais recente imediatamente após ela ter sido lançada, use um dos métodos a seguir.

2. Manualmente, por meio de download e instalação de uma versão mais recente sobre a instalação anterior.
   No início da instalação, é possível optar por preservar as configurações atuais do programa marcando a caixa de seleção **Utilizar configurações atuais**.

3. Manualmente, através da implementação automática em um ambiente de rede usando o ESET Remote Administrator.

## 2.5 Rastreamento do computador

Após instalar o ESET Endpoint Security, você deve executar um rastreamento do computador para verificar se há código malicioso. Na janela principal do programa, clique em **Rastreamento do computador** e, em seguida, clique em **Rastreamento inteligente**. Para obter mais informações sobre rastreamentos do computador, consulte a seção Rastreamento do computador.

# 3. Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET Endpoint Security e de suas configurações básicas.

## 3.1 Introdução ao design da interface do usuário

A janela principal do ESET Endpoint Security é dividida em duas seções principais. A primeira janela à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

A seguir, há uma descrição das opções dentro do menu principal:

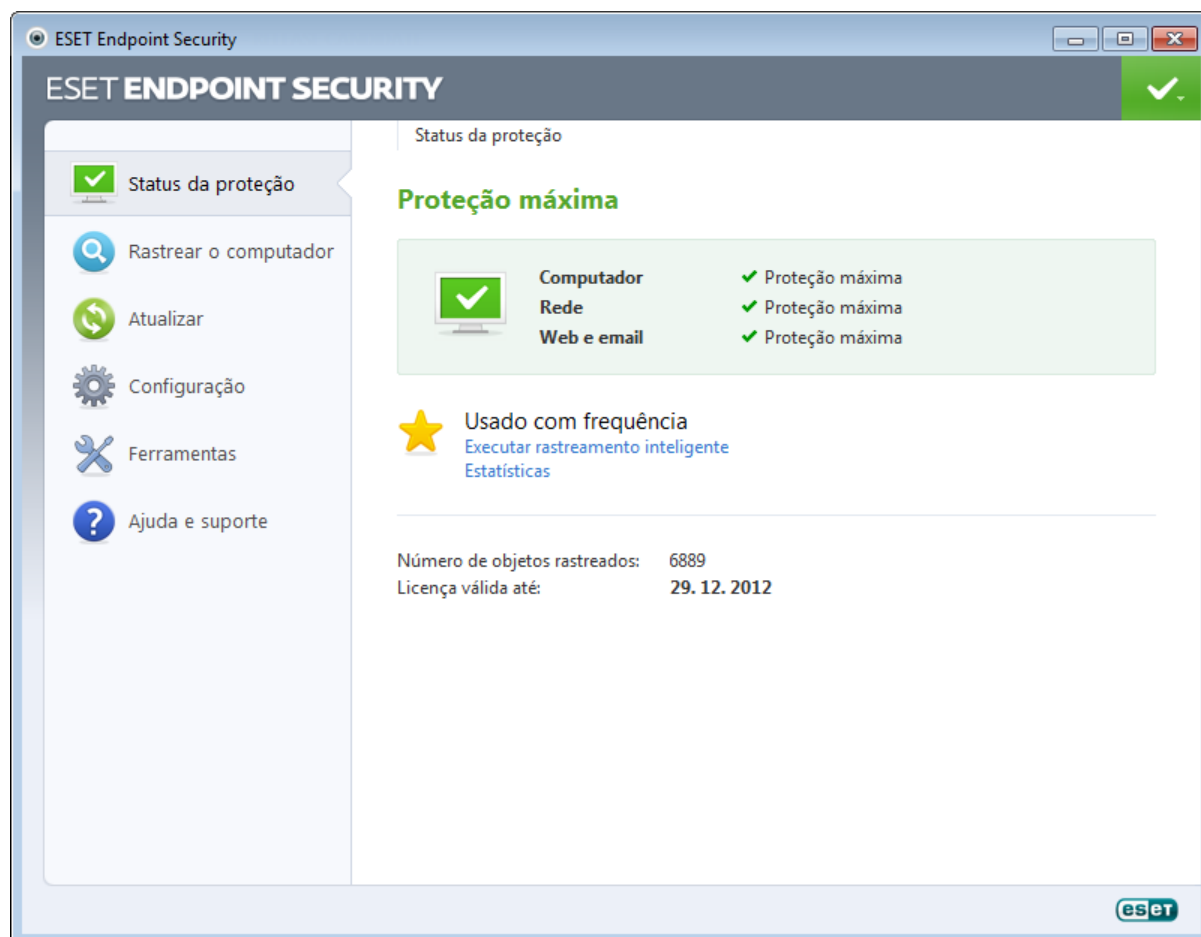
**Status da proteção** - Fornece informações sobre o status da proteção do ESET Endpoint Security.

**Rastrear o computador** – Essa opção permite que você configure e inicie o Rastreamento inteligente ou o Rastreamento personalizado.

**Atualizar** - Exibe informações sobre as atualizações do banco de dados de assinatura de vírus.

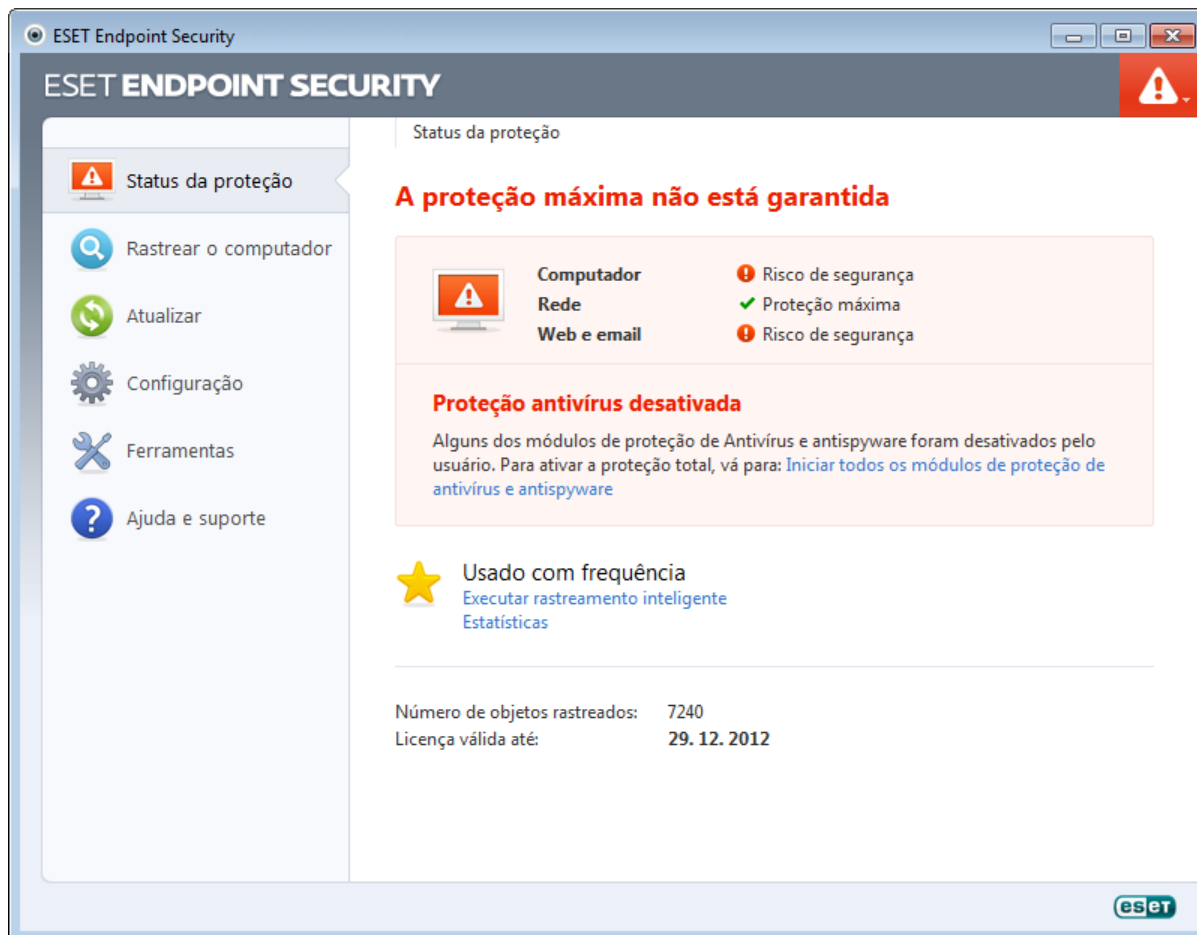
**Configuração** - Selecione essa opção para ajustar o nível de segurança do computador, da Web e do email e da rede .

**Ferramentas** - Fornece acesso a arquivos de log, estatísticas de proteção, monitoramento de atividade, processos em execução, conexões de rede, Agenda, quarentena, ESET SysInspector e ESET SysRescue.

**Ajuda e suporte** - Fornece acesso às páginas da ajuda, à Base de conhecimento da ESETe ao site e links da ESET para abrir uma solicitação de suporte ao Atendimento ao cliente.

A tela **Status da proteção** informa sobre a segurança e o nível de proteção atual do seu computador. O ícone verde de status de **Proteção máxima** indica que a proteção máxima está garantida.

A janela de status também exibe os recursos mais usados do ESET Endpoint Security. As informações sobre a data de expiração do programa também podem ser encontradas aqui.

## 3.2 O que fazer se o programa não funcionar adequadamente

Se os módulos ativados estiverem funcionando adequadamente, um ícone de marcação verde será atribuído a eles. Caso contrário, um ponto de exclamação vermelho ou um ícone de notificação laranja será exibido. Informações adicionais sobre o módulo serão mostradas na parte superior da janela. Uma solução sugerida para corrigir o módulo também é exibida. Para alterar o status dos módulos individuais, clique em **Configuração** no menu principal e clique no módulo desejado.

O ícone vermelho assinala problemas críticos - a proteção máxima do seu computador não está garantida. As possíveis razões são:

- Proteção em tempo real do sistema de arquivos desativada
- Firewall pessoal desativado
- Banco de dados de assinatura de vírus desatualizado
- Produto não ativado
- A licença do produto expirou

O ícone laranja indica que a Proteção do cliente de email ou de acesso à web está desativada, que há um problema com a atualização do programa (banco de dados de assinatura de vírus desatualizado, impossível atualizar) ou que a data de expiração da licença está se aproximando.

**Proteção antivírus e antispyware desativada** - Esse problema é assinalado por um ícone vermelho e uma notificação de segurança próxima ao item **Computador**. Você pode reativar a proteção antivírus e antispyware clicando em **Iniciar todos os módulos de proteção antivírus e antispyware**.

**Proteção do acesso à web desativada** - Esse problema é assinalado por um ícone laranja com um "i" e o status **Notificação de segurança**. É possível reativar Proteção do acesso à web clicando na notificação de segurança e em **Ativar proteção do acesso à Web**.

**Firewall pessoal do ESET desativado** - Esse problema é assinalado por um ícone vermelho e uma notificação de segurança próxima ao item **Rede**. Você pode reativar a proteção da rede clicando em **Ativar modo de filtragem**.

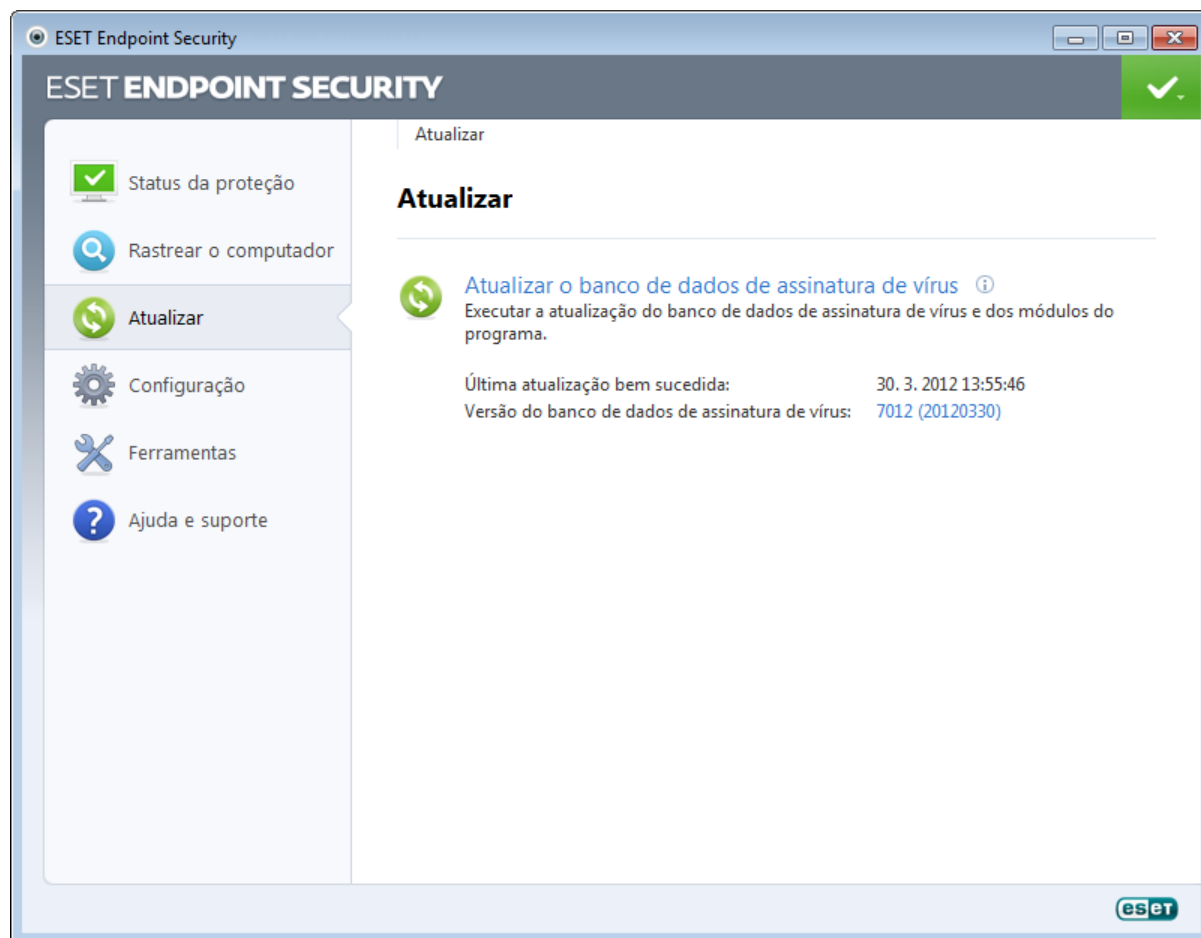
**Sua licença expirará em breve** - Isso é indicado pelo ícone do status de proteção exibindo um ponto de exclamação. Depois que a licença expirar, o programa não poderá ser atualizado e o ícone do status da proteção ficará vermelho.

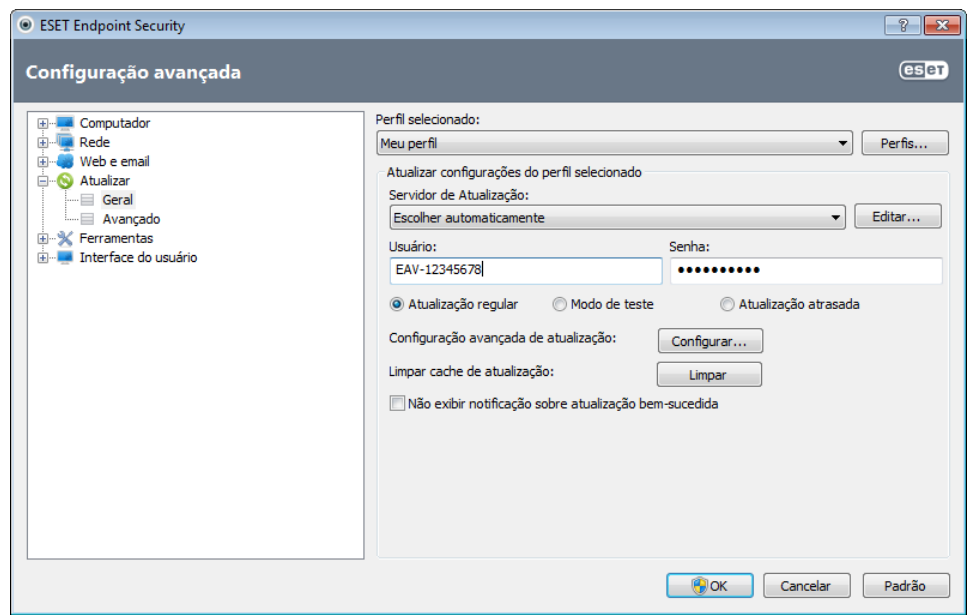
**Licença expirada** – Isso é indicado pelo ícone do status de proteção que fica vermelho. O programa não pode ser atualizado após a licença expirar. Recomendamos que você siga as instruções da janela de alerta para renovar sua licença.

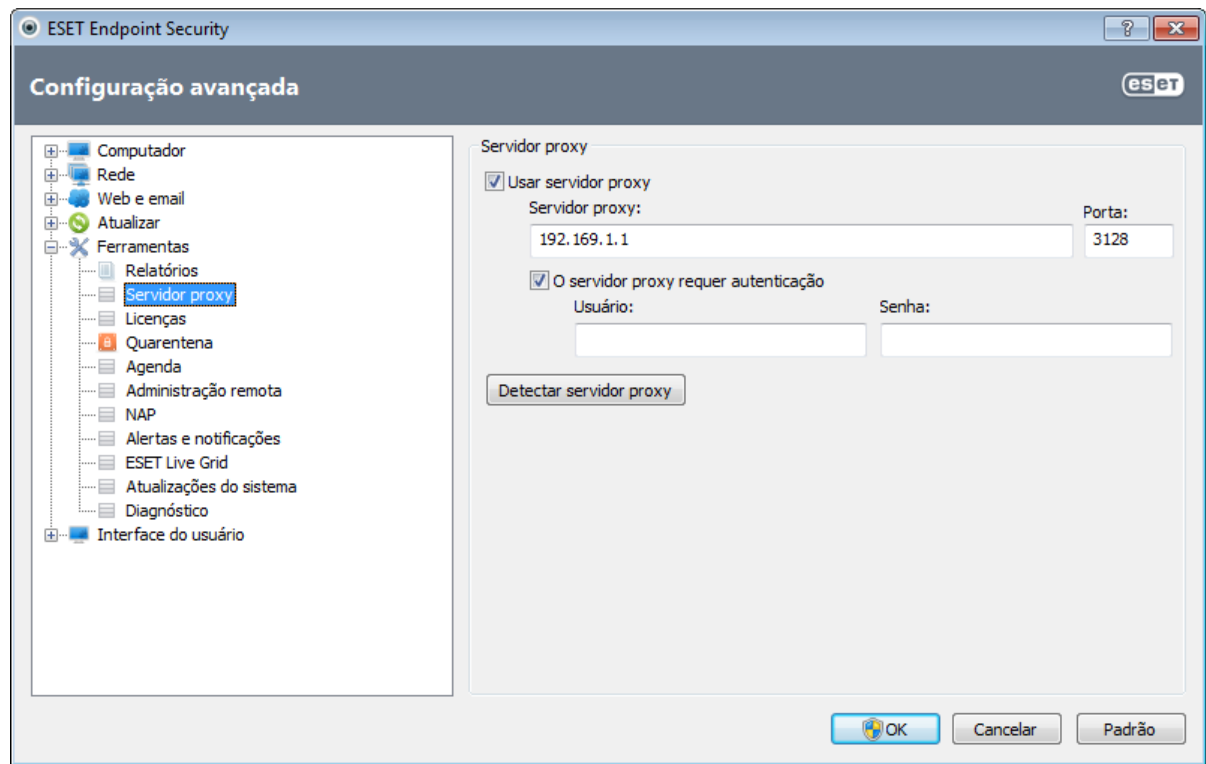
Se não for possível solucionar um problema com as soluções sugeridas, clique em **Ajuda e suporte** para acessar os arquivos de ajuda ou pesquisar na Base de conhecimento da ESET. Se precisar de assistência, entre em contato com o Atendimento ao Cliente da ESET. O Atendimento ao Cliente da ESET responderá rapidamente às suas dúvidas e o ajudará a encontrar uma solução.

## 3.3 Configuração da atualização

A atualização do banco de dados da assinatura de vírus e a atualização dos componentes do programa são partes importantes no fornecimento de proteção completa contra códigos maliciosos. Preste bastante atenção à sua configuração e operação. No menu principal, selecione **Atualizar** e clique em **Atualizar banco de dados de assinatura de vírus** para verificar se há uma atualização mais recente do banco de dados.

Se o nome de usuário e a senha não foram inseridos durante o processo de instalação do ESET Endpoint Security, você será solicitado a inseri-los neste momento.

ESET Endpoint Security
ESET ENDPOINT SECURITY
Status da proteção
Rastrear o computador
Atualizar
Configuração
Ferramentas
Ajuda e suporte
Atualizar
Atualizar
Atualizar o banco de dados de assinatura de vírus
Executar a atualização do banco de dados de assinatura de vírus e dos módulos do programa.
Última atualização bem sucedida: 30. 3. 2012 13:55:46
Versão do banco de dados de assinatura de vírus: 7012 (20120330)
eset

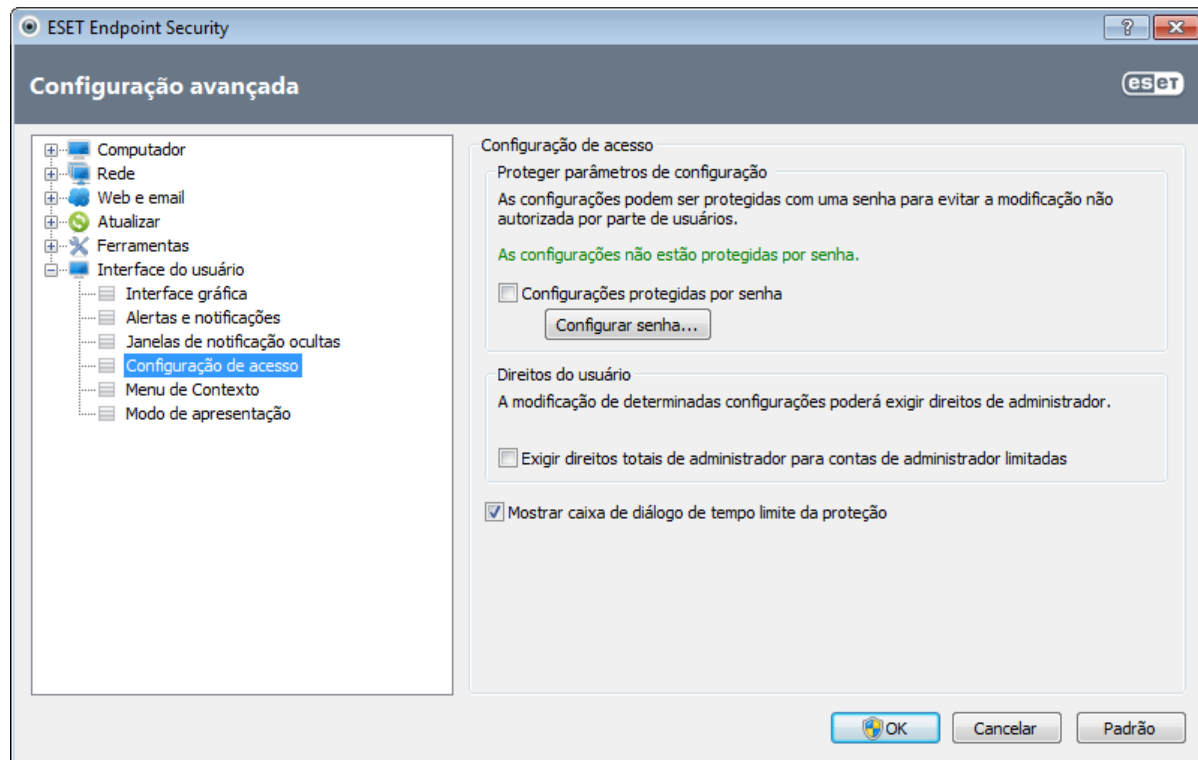
A janela Configuração avançada (no menu principal, clique em **Configuração** e escolha a opção **Entrar na configuração avançada...**, ou pressione F5 no teclado) contém opções de atualização adicionais. Clique em **Atualizar** na árvore Configuração avançada à esquerda. O menu suspenso **Atualizar servidor** estará configurado como **Escolher automaticamente** por padrão. Para configurar as opções avançadas de atualização, como o modo de atualização, o acesso ao servidor proxy, as conexões de rede e a criação de cópias do banco de dados de assinatura de vírus, clique no botão **Configuração...**.

## 3.4 Configuração do servidor proxy

Se você utilizar um servidor proxy para controlar a conexão com a Internet em um sistema utilizando o ESET Endpoint Security, ele deve ser especificado na Configuração avançada. Para acessar a janela de configuração do servidor proxy, pressione F5 para abrir a janela Configuração avançada e clique em **Ferramentas** > **Servidor proxy** na árvore Configuração avançada. Selecione a opção **Utilizar servidor proxy** e preencha os campos **Servidor proxy** (endereço IP) e **Porta**. Se necessário, selecione a opção **O servidor proxy requer autenticação** e insira o **Nome de usuário** e a **Senha**.

Se essas informações não estiverem disponíveis, você pode tentar detectar automaticamente as configurações do servidor proxy clicando no botão **Detectar servidor proxy**.

**OBSERVAÇÃO:** As opções de servidor proxy para diferentes perfis de atualização podem variar. Se for este o caso,

configure os diferentes perfis de atualização na Configuração avançada, clicando em **Atualizar** na árvore Configuração avançada.

## 3.5 Proteção de configurações

As configurações do ESET Endpoint Security podem ser muito importantes da perspectiva da sua política de segurança. Modificações não autorizadas podem colocar em risco a estabilidade e a proteção do seu sistema. Para proteger com senha os parâmetros de configuração, acesse o menu principal e clique em **Configuração** > **Entrar na configuração avançada...** > **Interface do usuário** > **Configuração de acesso**, selecione a opção **Configurações protegidas por senha** e clique no botão **Configurar senha...**



Insira uma senha nos campos **Nova senha** e **Confirmar nova senha** e clique em **OK**. Esta senha será solicitada em todas as configurações futuras que forem realizadas no ESET Endpoint Security.

## 3.6 Configuração de zona Confiável

É necessário configurar a Zona confiável para proteger o computador em um ambiente de rede. É possível permitir que outros usuários acessem o seu computador configurando a Zona confiável e permitindo o compartilhamento. Clique em **Configuração** > **Rede** > **Alterar o modo de proteção do seu computador na rede...** Uma janela exibirá as opções que permitem escolher o modo de proteção desejado do seu computador na rede.

A detecção de zona confiável ocorre após a instalação do ESET Endpoint Security e sempre que o seu computador se conectar a uma nova rede, portanto, na maioria dos casos não há necessidade de definir a Zona confiável. Por padrão, há uma janela da caixa de diálogo exibida na detecção de uma nova zona que permite configurar o nível de proteção dessa zona.

ESET Endpoint Security

Nova conexão de rede detectada

Escolha o modo de proteção do computador na rede:
Sub-rede: 10.0.2.0 / 255.255.255.0
Sufixo DNS: hq.eset.com
Endereços DHCP: 10.0.2.2

Proteção rígida – Rede pública
O seu computador não estará visível para outros computadores na rede (ou seja, suas pastas ou impressoras compartilhadas não estarão visíveis de outros computadores na rede). Um exemplo desse tipo de conexão é uma rede pública.

Permitir compartilhamento - Rede doméstica
O seu computador estará visível para outros computadores na rede (ou seja, suas pastas ou impressoras compartilhadas estarão visíveis para outros computadores na rede). Um exemplo desse tipo de conexão é a rede doméstica ou de escritório.

O modo selecionado pode ser alterado posteriormente na seção Configuração
Configuração avançada...

Cancelar

**Aviso:** Uma configuração incorreta da zona confiável pode representar um risco de segurança para o seu computador.

**OBSERVAÇÃO:** Por padrão, as estações de trabalho de uma Zona confiável têm acesso garantido a arquivos e impressoras compartilhados, a comunicação RPC de entrada é ativada e o compartilhamento da área de trabalho remota é disponibilizado.

# 4. Trabalhar com o ESET Endpoint Security

As opções de configuração do ESET Endpoint Security permitem ajustar os níveis de proteção do computador e da rede.

O menu **Configuração** contém as seguintes opções:

- **Computador**
- **Rede**
- **Web e email**

Clique em qualquer componente para ajustar as configurações avançadas do módulo de proteção correspondente.

A configuração da proteção do **Computador** permite ativar ou desativar os seguintes componentes:

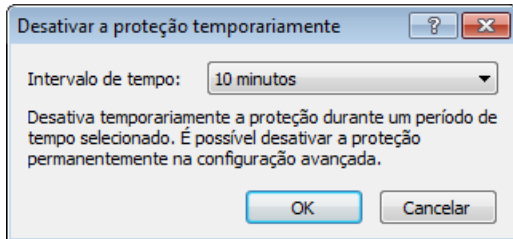
- **Proteção em tempo real do sistema de arquivos** – Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador.
- **Proteção de documentos** - O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, como, por exemplo, elementos do Microsoft ActiveX.
- **Controle de dispositivos** - Esse módulo permite rastrear, bloquear ou ajustar filtros/permissões estendidos e seleciona como o usuário pode acessar e trabalhar com um determinado dispositivo (CD/DVD/USB...).
- **HIPS** - O sistema HIPS monitora os eventos dentro do sistema operacional e reage a eles de acordo com um conjunto de regras personalizado.
- **Modo de apresentação** - Ativa ou desativa o Modo de apresentação. Você receberá uma mensagem de aviso (risco potencial de segurança) e a janela principal será exibida em laranja após a ativação do Modo de apresentação.
- **Proteção Anti-Stealth** - Fornece a detecção de programas nocivos, como os rootkits, que podem se auto-ocultar do sistema operacional. Isso significa que não é possível detectá-los usando técnicas comuns de testes.

A seção **Rede** permite ativar ou desativar o **Firewall pessoal**.

A configuração da proteção **Web e email** permite ativar ou desativar os seguintes componentes:

- **Proteção do acesso à web** - Se ativada, todo o tráfego através de HTTP ou HTTPS será rastreado quanto a software malicioso.
- **Proteção do cliente de email** - Monitora a comunicação recebida através dos protocolos POP3 e IMAP.
- **Proteção antispam** - Rastreia emails não solicitados (também conhecidos como spams).
- **Controle de Web** - Bloqueia páginas da web que possam conter material potencialmente ofensivo. Além disso, os empregadores ou administradores do sistema podem proibir o acesso a até 27 categorias de sites predefinidas.

**OBSERVAÇÃO:** A Proteção de documentos será exibida após a ativação da opção (**Entrar na configuração avançada...** (F5) > **Computador** > **Antivírus e antispyware** > **Proteção de documentos** > **Integrar ao sistema**).

Depois de clicar em **Ativado**, a caixa de diálogo **Desativar a proteção temporariamente** é exibida. Clique em **OK** para desativar o componente de segurança selecionado. O menu suspenso **Intervalo de tempo** representa o período de tempo em que o componente selecionado será desativado.



Para reativar a proteção do componente de segurança desativado, clique em **Desativado**.

**OBSERVAÇÃO:** Ao desabilitar a proteção usando este método, todas as partes com deficiência de proteção serão ativadas após a reinicialização do computador.

Existem opções adicionais na parte inferior da janela de configuração. Para carregar os parâmetros de configuração utilizando um arquivo de configuração .xml ou salvar os parâmetros atuais em um arquivo de configuração, use a opção **Importar e exportar configurações...**.

## 4.1 Computador

O módulo **Computador** pode ser encontrado no painel **Configuração** depois de clicar em **Computador**. Essa janela mostra uma visão geral de todos os módulos de proteção. Para desativar os módulos individuais temporariamente, clique em **Desativar** embaixo de cada módulo. Observe que essa ação pode diminuir a proteção do seu computador. Para acessar as configurações detalhadas para cada módulo, clique em **Configurar...**.

Clique em **Editar exclusões...** para abrir a janela de configuração Exclusão, que permite a exclusão de arquivos e pastas do rastreamento.

**Desativar temporariamente a proteção antivírus e antispyware** - Desativa todos os módulos de proteção antivírus e antispyware. A caixa de diálogo **Desativar a proteção temporariamente** com o menu suspenso **Intervalo de tempo** será exibida. O menu suspenso **Intervalo de tempo** representa o período de tempo em que a proteção será desativada. Clique em **OK** para confirmar.

**Configuração do rastreamento do computador...** - Clique para ajustar os parâmetros do Scanner sob demanda (rastreamento executado manualmente).

### 4.1.1 Proteção antivírus e antispyware

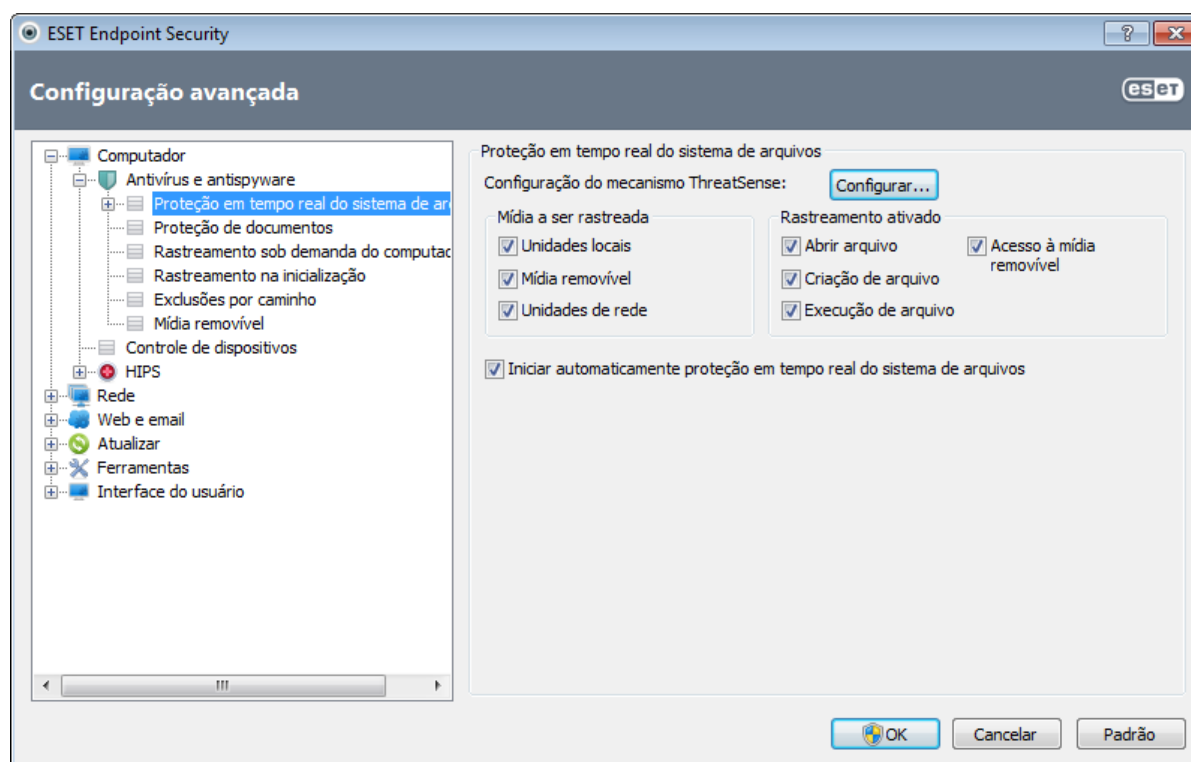
A proteção de antivírus e antispyware protege contra ataques de sistemas maliciosos ao controlar arquivos, emails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la, primeiro bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena.

### 4.1.1.1 Proteção em tempo real do sistema de arquivos

A proteção em tempo real do sistema de arquivos controla todos os eventos relacionados a antivírus no sistema. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção em tempo real do sistema de arquivos é ativada na inicialização do sistema.

A proteção em tempo real do sistema de arquivos verifica todos os tipos de mídia e é acionada por vários eventos do sistema, tais como o acesso a um arquivo. Com a utilização dos métodos de detecção da tecnologia ThreatSense (descritos na seção Configuração de parâmetros do mecanismo ThreatSense ), a proteção em tempo real do sistema de arquivos pode variar para arquivos recém-criados e existentes. Em arquivos recém-criados, é possível aplicar um nível mais profundo de controle.

Para proporcionar o impacto mínimo no sistema ao usar a proteção em tempo real, os arquivos que já foram rastreados não são rastreados repetidamente (exceto se tiverem sido modificados). Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus. Esse comportamento é configurado usando a **Otimização inteligente**. Se esse recurso for desativado, todos os arquivos serão rastreados toda vez que forem acessados. Para modificar essa opção, pressione F5 para abrir a janela Configuração avançada e clique em **Computador** > **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos** na árvore Configuração avançada. Depois, clique no botão **Configuração...** ao lado de **Configuração de parâmetros do mecanismo ThreatSense**, clique em **Outros** e marque ou desmarque a opção **Ativar otimização inteligente**.

Por padrão, a proteção em tempo real do sistema de arquivos é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outra proteção em tempo real), a proteção em tempo real pode ser encerrada desmarcando a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos**.

#### 4.1.1.1.1 Mídia a ser rastreada

Por padrão, todos os tipos de mídia são rastreadas quanto a potenciais ameaças.

**Unidades locais** - Controla todas as unidades de disco rígido do sistema.

**Mídia removível** - Disquetes, CD/DVDs, dispositivos de armazenamento USB, etc.

**Unidades de rede** - Rastreia todas as unidades mapeadas.

Recomendamos manter as configurações padrão e modificá-las somente em casos específicos, como quando o rastreamento de determinada mídia tornar muito lenta a transferência de dados.

#### 4.1.1.1.2 Rastreamento ativado (Rastreamento disparado por evento)

Por padrão, todos os arquivos são verificados na abertura, criação ou execução. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador.

**Abertura de arquivo** - Ativa ou desativa o rastreamento de arquivos abertos.

**Criação de arquivo** - Ativa ou desativa o rastreamento dos arquivos criados ou modificados recentemente.

**Execução de arquivo** - Ativa ou desativa o rastreamento de arquivos executados.

**Acesso à mídia removível** - Ativa ou desativa o rastreamento disparado ao acessar mídia removível em particular com espaço de armazenamento.

#### 4.1.1.1.3 Opções de rastreamento avançadas

Opções de configuração mais detalhadas podem ser encontradas em **Computador** > **Antivírus e antispyware** > **Proteção do sistema em tempo real** > **Configuração avançada**.

**Parâmetros ThreatSense adicionais para arquivos criados e modificados recentemente** - A probabilidade de infecção em arquivos criados ou modificados recentemente é comparativamente maior do que nos arquivos existentes. Por esse motivo, o programa verifica esses arquivos com parâmetros de rastreamento adicionais. Além dos métodos comuns de rastreamento baseados em assinaturas, é usada a heurística avançada, que aumenta enormemente os índices de detecção uma vez que ela detecta novas ameaças antes do lançamento da atualização do banco de dados de assinatura de vírus. Além dos arquivos recém-criados, o rastreamento também é executado em arquivos de autoextração (.sfx) e em empacotadores em tempo real (arquivos executáveis compactados internamente). Por padrão, os arquivos compactados são rastreados até o décimo nível de compactação e são verificados, independentemente do tamanho real deles. Para modificar as configurações de rastreamento em arquivos compactados, desmarque a opção **Configurações padrão de rastreamento em arquivos compactados**.

**Parâmetros ThreatSense adicionais para arquivos executados** - Por padrão, a heurística avançada não é usada quando os arquivos são executados. Entretanto, em alguns casos pode ser necessário ativar essa opção (marcando a opção **Heurística avançada na execução de arquivos**). Observe que a heurística avançada pode tornar mais lenta a execução de alguns programas devido ao aumento dos requisitos do sistema. Enquanto a opção **Heurística avançada na execução de arquivos de dispositivos externos** estiver ativada, se você desejar excluir algumas portas (USB) de mídia removível de serem rastreadas pela heurística avançada na execução do arquivo, clique em **Exceções...** para abrir a janela de exclusões da unidade de mídia removível. A partir daqui, você poderá personalizar as configurações marcando ou desmarcando as caixas de seleção que representam cada porta.

#### 4.1.1.1.4 Níveis de limpeza

A proteção em tempo real possui três níveis de limpeza (para acessar, clique no botão **Configuração...** na seção **Proteção em tempo real do sistema de arquivos** e clique na ramificação **Limpeza**).

**Sem limpeza** - Os arquivos infectados não serão limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.

**Limpeza padrão** - O programa tentará limpar ou excluir automaticamente um arquivo infectado com base em uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma mensagem de informação localizada no canto inferior direito da tela. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá uma seleção de ações de acompanhamento. O mesmo ocorre quando uma ação predefinida não pode ser concluída.

**Limpeza rígida** - O programa limpará ou excluirá todos os arquivos infectados. As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, o usuário é solicitado a selecionar uma ação em uma janela de aviso.

**Aviso:** Se um arquivo compactado tiver um ou mais arquivos infectados, haverá duas opções para tratar o arquivo. No modo padrão (Limpeza padrão), o arquivo completo será excluído se todos os arquivos que ele contém forem arquivos infectados. No modo **Limpeza rígida**, o arquivo compactado seria excluído se tiver, pelo menos, um arquivo infectado, qualquer que seja o status dos outros arquivos no arquivo compactado.

#### 4.1.1.1.5 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Seja sempre cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos. Por exemplo, se houver um conflito com um certo aplicativo ou rastreador em tempo real de outro programa antivírus.

Após a instalação do ESET Endpoint Security, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique no botão **Padrão** localizado na parte inferior direita da janela **Proteção em tempo real do sistema de arquivos** (**Configuração avançada** > **Computador** > **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos**).

#### 4.1.1.1.6 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.com. Este arquivo de teste é especial, inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus. O arquivo eicar.com está disponível para download em http://www.eicar.org/download/eicar.com

**OBSERVAÇÃO:** Antes de realizar um rastreamento da proteção de tempo real, é preciso desativar o firewall. Se o firewall estiver ativado, ele detectará e impedirá o download do arquivo de teste.

#### 4.1.1.1.7 O que fazer se a proteção em tempo real não funcionar

Neste capítulo, descrevemos situações problemáticas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

**Proteção em tempo real desativada**

Se a proteção em tempo real foi inadvertidamente desativada por um usuário, é preciso reativá-la. Para reativar a proteção em tempo real, navegue até **Configuração** na janela principal do programa e clique em **Proteção em tempo real do sistema de arquivos**.

Se a proteção em tempo real não for ativada na inicialização do sistema, geralmente é porque a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está desativada. Para ativar essa opção, navegue até Configuração avançada (F5) e clique em **Computador** > **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos** na árvore Configuração avançada. Na seção **Configuração avançada** na parte inferior da janela, certifique-se de que a caixa de seleção **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está marcada.

**Se a proteção em tempo real não detectar nem limpar infiltrações**

Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema.

#### A proteção em tempo real não é iniciada

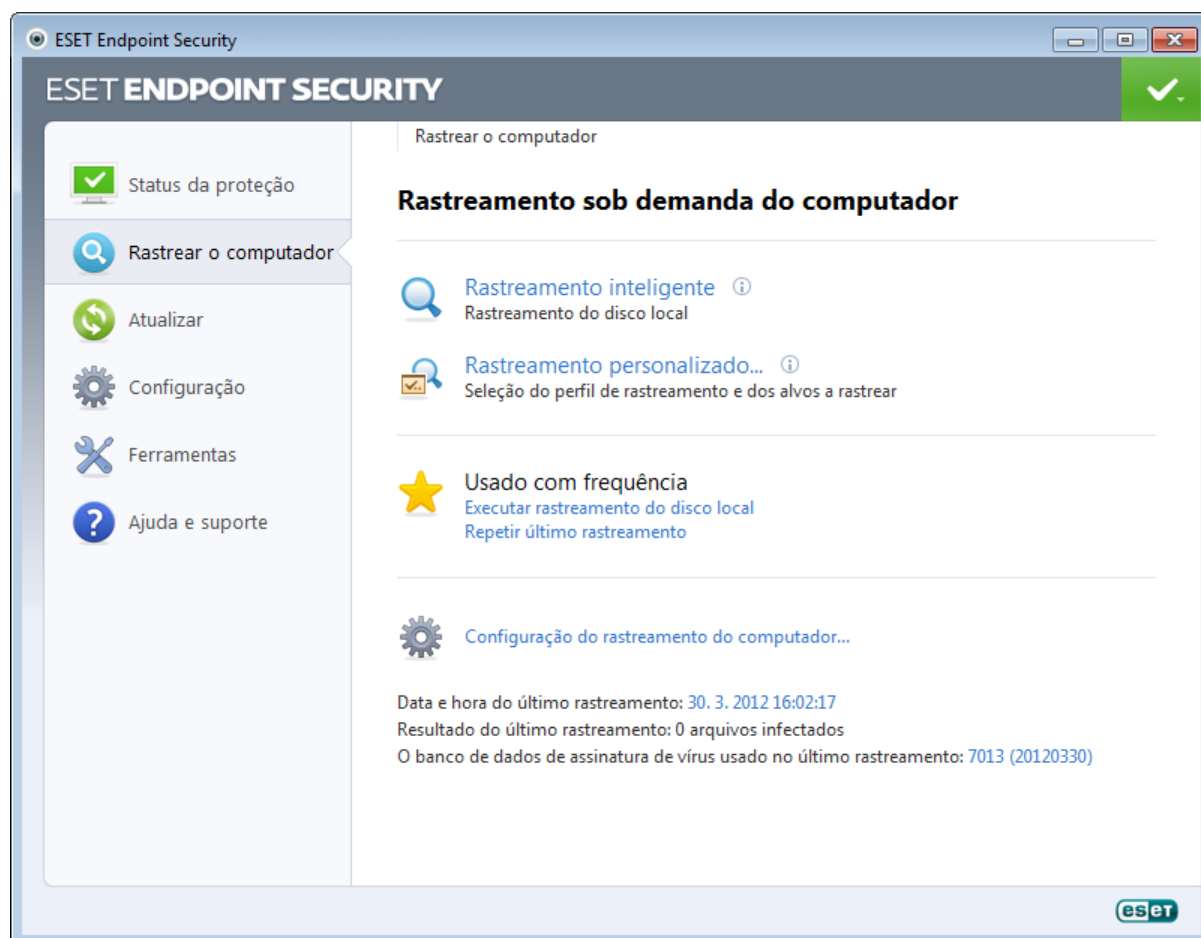
Se a proteção em tempo real não for ativada na inicialização do sistema (e estiver ativada a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos**), isto pode ser devido a conflitos com outros programas. Se for este o caso, entre em contato com o Atendimento ao Cliente da ESET.

### 4.1.1.2 Proteção de documentos

O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, tais como elementos do Microsoft ActiveX. **Integrar ao sistema** ativa o sistema de proteção. Para modificar essa opção, pressione F5 para abrir a janela Configuração avançada e clique em **Compuador** > **Antivírus e antispyware** > **Proteção de documentos** na árvore Configuração avançada. Quando ativada, a Proteção de documentos pode ser visualizada na janela principal do ESET Endpoint Security em **Configuração** > **Computador**.

Este recurso é ativado por aplicativos que utilizam o Microsoft Antivirus API (por exemplo, Microsoft Office 2000 e superior ou Microsoft Internet Explorer 5.0 e superior).

### 4.1.1.3 Rastreamento do computador

O rastreador sob demanda é uma parte importante da sua solução antivírus. Ele é usado para realizar rastreamentos nos arquivos e pastas do seu computador. Do ponto de vista da segurança, é fundamental que os rastreamentos do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. Recomendamos que você realize rastreamentos detalhados regulares do sistema para detectar vírus que não tenham sido capturados pela Proteção em tempo real do sistema de arquivos quando foram gravados no disco. Isso pode acontecer se a Proteção em tempo real do sistema de arquivos estiver desativada no momento, se o banco de dados de vírus for obsoleto ou se o arquivo não for detectado como vírus ao ser salvo no disco.

Há dois tipos de **Rastreamento do computador** disponíveis. O **Rastreamento inteligente** rastreia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

Leia o capítulo Progresso do rastreamento para obter mais informações sobre o processo de rastreamento.

Recomendamos que execute um rastreamento do computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Agenda**.

### 4.1.1.3.1 Tipos de rastreamento

#### 4.1.1.3.1.1 Rastreamento inteligente

O Rastreamento inteligente permite que você inicie rapidamente um rastreamento do computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. A vantagem do Rastreamento inteligente é que ele é fácil de operar e não requer configuração de rastreamento detalhada. O Rastreamento inteligente verifica todos os arquivos nas unidades locais e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte a seção Limpeza.

#### 4.1.1.3.1.2 Rastreamento personalizado

O rastreamento personalizado é uma solução excelente, caso queira especificar parâmetros de rastreamento, como rastreamento de alvos e métodos de rastreamento. A vantagem do rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

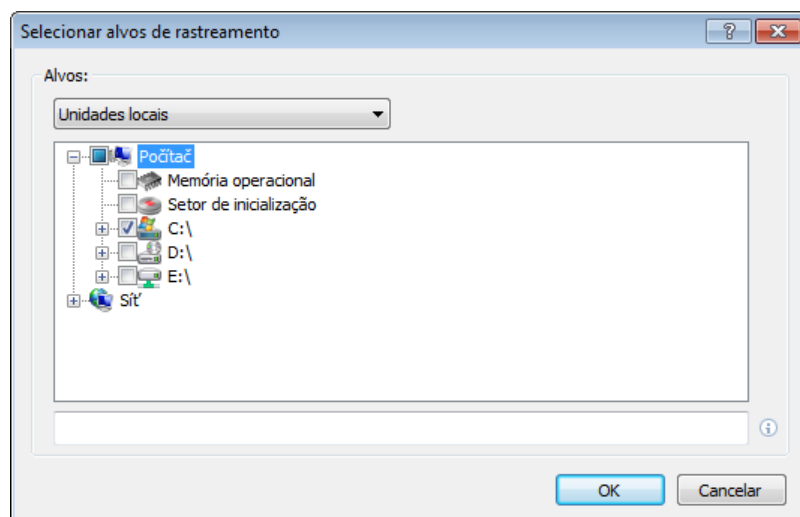
Para selecionar os alvos de rastreamento, selecione **Rastreamento do computador** > **Rastreamento personalizado** e selecione uma opção no menu suspenso **Alvos de rastreamento** ou selecione alvos específicos na estrutura em árvore. Um alvo de rastreamento pode ser também especificado por meio da inserção do caminho da pasta ou arquivo(s) que você deseja incluir. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione a opção **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração...** > **Limpeza**.

A realização de rastreamentos de computador com o Rastreamento personalizado é adequada para usuários avançados com experiência anterior na utilização de programas antivírus.

### 4.1.1.3.2 Alvos de rastreamento

A janela Alvos de rastreamento permite definir que objetos (memória, unidades, setores, arquivos e pastas) são rastreados quanto a infiltrações. O menu suspenso **Alvos de rastreamento** permite selecionar alvos de rastreamento predefinidos.

- **Por configurações de perfil** - Seleciona alvos definidos no perfil de rastreamento selecionado.
- **Mídia removível** - Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD.
- **Unidades locais** - Controla todas as unidades de disco rígido do sistema.
- **Unidades de rede** - Seleciona todas as unidades de rede mapeadas.
- **Nenhuma seleção** - Cancela todas as seleções.

Um alvo de rastreamento pode ser também especificado por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir no rastreamento. Selecione alvos na estrutura em árvore, que lista todos os dispositivos disponíveis no computador.

Para navegar rapidamente até um alvo de rastreamento selecionado ou para adicionar diretamente um alvo desejado,

digite-o no campo em branco embaixo da lista de pastas. Isso só é possível se nenhum alvo tiver sido selecionado na estrutura em árvore e se o menu **Alvos de rastreamento** estiver definido como **Nenhuma seleção**.

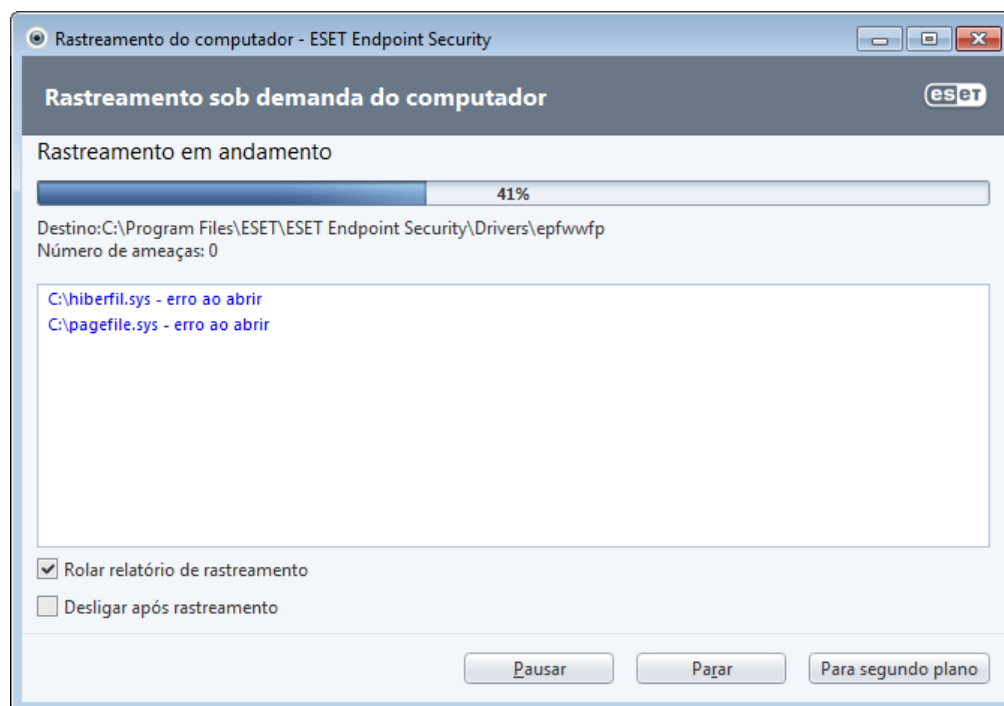
### 4.1.1.3.3 Perfis de rastreamento

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Computador** > **Antivírus e antispyware** > **Rastreamento do computador** > **Perfis...**. A janela **Perfis de configuração** inclui o menu suspenso **Perfil selecionado** que lista os perfis de rastreamento existentes e a opção para criar um novo. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense para obter uma descrição de cada parâmetro da configuração de rastreamento.

**Exemplo:** Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a **Limpeza rígida**. Na janela **Perfis de configuração**, clique no botão **Adicionar...**. Digite o nome do novo perfil no campo **Nome do perfil** e selecione **Rastreamento inteligente** no menu suspenso **Copiar configurações do perfil**. Depois, ajuste os demais parâmetros de maneira a atender as suas necessidades.

### 4.1.1.3.4 Progresso do rastreamento

A janela de progresso do rastreamento mostra o status atual do rastreamento e informações sobre a quantidade de arquivos encontrados que contêm código malicioso.

**OBSERVAÇÃO:** É normal que alguns arquivos, como arquivos protegidos por senha ou arquivos exclusivamente utilizados pelo sistema (geralmente pagefile.sys e determinados arquivos de log), não possam ser rastreados.

**Progresso do rastreamento** - A barra de progresso mostra o percentual de objetos já rastreados em relação aos objetos que ainda aguardam o rastreamento. O valor é derivado do número total de objetos incluídos no rastreamento..

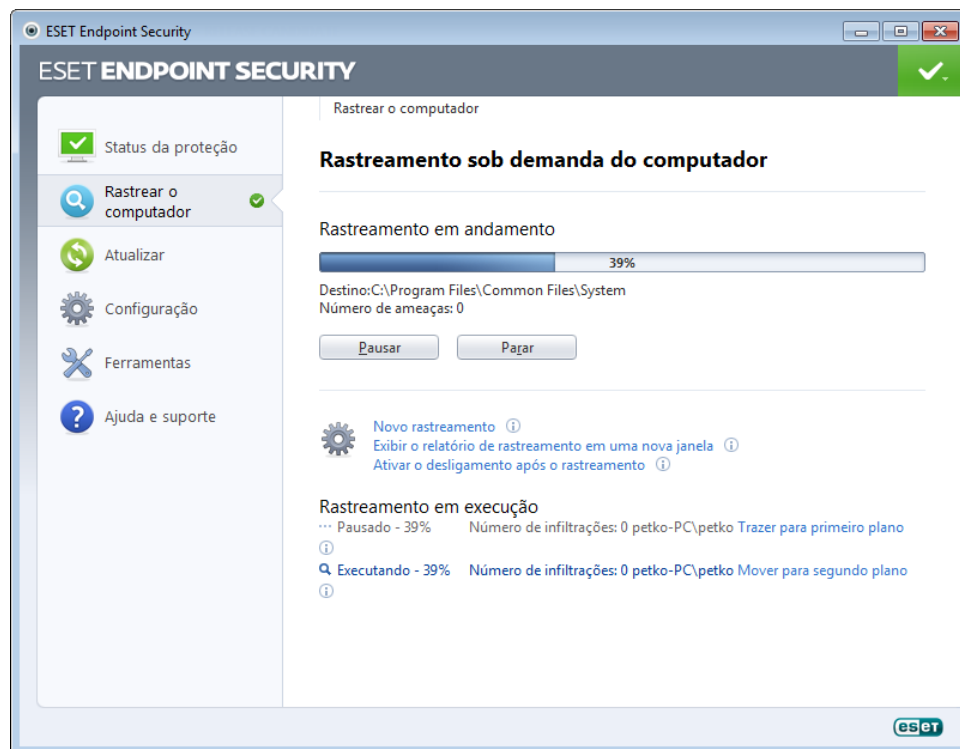
**Destino** - O nome do objeto rastreado no momento e sua localização.

**Número de ameaças** - Mostra o número total de ameaças encontradas durante um rastreamento.

**Pausa** - Pausa um rastreamento.

**Continuar** - Essa opção torna-se visível quando o progresso do rastreamento é pausado. Clique em **Continuar** para dar continuidade ao rastreamento.

**Parar** - Termina o rastreamento.

**Para segundo plano** - É possível executar outro rastreamento paralelamente. O rastreamento em execução será minimizado e ficará em segundo plano.

Clique em **Trazer para primeiro plano** para trazer um rastreamento para o primeiro plano e retornar ao processo de rastreamento.

**Percorrer log de rastreamento** - Se estiver ativado, o log de rastreamento rolará automaticamente para baixo à medida que novas entradas forem adicionadas para que as entradas mais recentes fiquem visíveis.

**Ativar o desligamento após o rastreamento** - Ativa um desligamento agendado quando o computador conclui o rastreamento sob demanda. Uma janela de diálogo de confirmação do desligamento aparece e permanece aberta por 60 segundos. Clique em **Cancelar** caso queira desativar o desligamento solicitado.

### 4.1.1.4 Rastreamento na inicialização

O rastreamento automático de arquivo na inicialização será executado na inicialização do sistema ou durante a atualização do banco de dados de assinatura de vírus. Esse rastreamento depende das Tarefas e configurações da agenda.

As opções de rastreamento na inicialização são parte de uma tarefa da agenda da **Rastreamento de arquivo na inicialização do sistema**. Para alterar suas configurações, acesse **Ferramentas** > **Agenda**, clique em **Rastreamento automático de arquivo na inicialização** e no botão **Editar...**. Na última etapa, a janela Rastreamento automático de arquivo na inicialização será exibida (consulte o capítulo a seguir para obter mais detalhes).

Para obter mais instruções sobre o gerenciamento e a criação de tarefas da Agenda, consulte Criação de novas tarefas.

#### 4.1.1.4.1 Rastreamento de arquivos em execução durante inicialização do sistema

O menu suspenso **Nível de rastreamento** especifica a profundidade do rastreamento da execução de arquivos na inicialização do sistema. Os arquivos são organizados em ordem crescente pelo número de arquivos a serem rastreados:

- **Somente os arquivos usados com mais frequência** (menos arquivos rastreados)
- **Arquivos usados com frequência**
- **Arquivos usados comumente**
- **Arquivos usados raramente**
- **Todos os arquivos registrados** (mais arquivos rastreados)

Dois grupos específicos de **Nível de rastreamento** também estão inclusos:

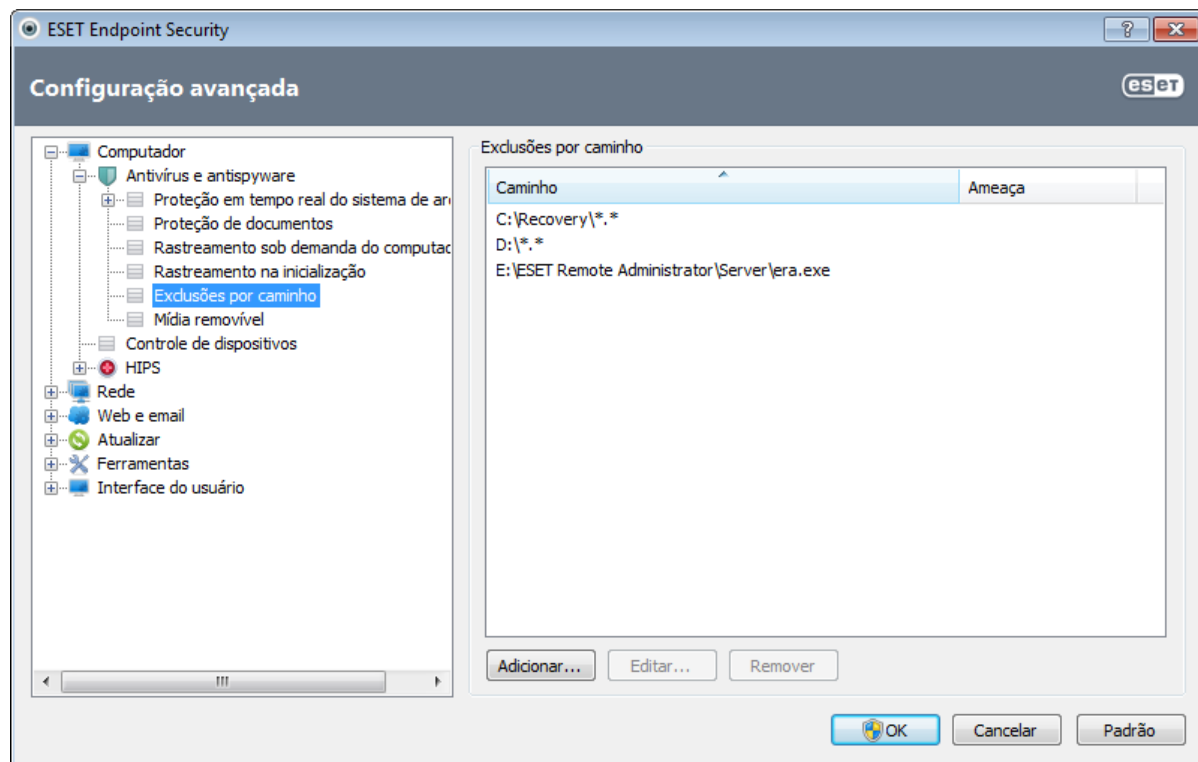
- **Arquivos executados antes do logon do usuário** - Contém arquivos de locais que permitem que esses arquivos sejam executados sem que o usuário esteja conectado em (inclui quase todos os locais de inicialização, tais como serviços, objetos auxiliares do navegador, notificação de Winlogon, entradas da Agenda do Windows, dlls conhecidos, etc.).
- **Arquivos executados após o logon do usuário** - Contém arquivos de locais que permitem a execução desses arquivos apenas após um usuário se conectar (inclui arquivos que são executados somente para um usuário específico, normalmente arquivos em HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run)

As listas de arquivos a serem rastreados estão fixas para cada grupo.

**Prioridade de rastreamento** - Um nível de prioridade a ser usado para início do rastreamento:

- **Normal** - em uma carga média do sistema,
- **Baixa** - em uma carga baixa do sistema,
- **Mais baixa** - quando a carga do sistema é a menor possível,
- **Quando em espera** - a tarefa será realizada somente quando o sistema estiver em espera.

### 4.1.1.5 Exclusões por caminho

As exclusões permitem que você exclua arquivos e pastas do rastreamento. Não recomendamos que você altere essas opções, a fim de garantir que todos os objetos sejam rastreados contra ameaças. Entretanto, existem situações em que você precisará excluir um objeto. Por exemplo, entradas extensas do banco de dados que diminuem o desempenho do computador durante o rastreamento ou um software que entra em conflito com a verificação.

**Caminho** - caminho para arquivos e pastas excluídos.

**Ameaça** - se houver um nome de uma ameaça próximo a um arquivo excluído, significa que o arquivo só foi excluído para a determinada ameaça, e não completamente. Portanto, se o arquivo for infectado posteriormente com outro malware, ele será detectado pelo módulo antivírus. Esse tipo de exclusão pode ser utilizado apenas para determinados tipos de infiltrações e pode ser criado na janela de alerta de ameaças que informa a infiltração (clique em **Mostrar opções avançadas** e selecione **Excluir da detecção**) ou em **Configuração** > **Quarentena** utilizando a opção do menu de contexto **Restaurar e excluir da detecção** no arquivo em quarentena.

**Adicionar...** - exclui objetos da detecção.

**Editar...** - permite que você edite as entradas selecionadas.

**Remover** - remove as entradas selecionadas.

Para excluir um objeto do rastreamento:

1. Clique em **Adicionar...**,
2. Digite o caminho para um objeto ou selecione-o na estrutura em árvore.

Você pode usar caracteres curinga para abranger um grupo de arquivos. Um ponto de interrogação (?) representa um caractere de variável único e um asterisco (*) representa uma cadeia de caracteres variável, com zero ou mais caracteres.

**Exemplos**

- Se você desejar excluir todos os arquivos em uma pasta, digite o caminho para a pasta e use a máscara "*.*".
- Para excluir a unidade por completo, incluindo todos os arquivos e subpastas, use a máscara "D:*".
- Se você desejar excluir somente arquivos doc, use a máscara "*.doc".
- Se o nome de um arquivo executável tiver um determinado número de caracteres (e os caracteres variarem) e você souber somente o primeiro com certeza (digamos, "D"), use o seguinte formato: "D????.exe". Os sinais de interrogação substituem os caracteres em falta (desconhecidos).

### 4.1.1.6 Configuração de parâmetros do mecanismo ThreatSense

O ThreatSense é a tecnologia que consiste em muitos métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante as primeiras horas da propagação de uma nova ameaça. Ela utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina os rootkits com êxito.

As opções de configuração da tecnologia ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados.
- A combinação de diversos métodos de detecção.
- Níveis de limpeza etc.

Para acessar a janela de configuração, clique no botão **Configuração...** localizado na janela de configuração de qualquer módulo que use a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- Proteção em tempo real do sistema de arquivos,
- Proteção de documentos,
- Proteção do cliente de email,
- Proteção do acesso à web,
- e Rastreamento do computador.

Os parâmetros do ThreatSense são altamente otimizados para cada módulo, e modificá-los pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre verificar empacotadores em tempo real ou ativar a heurística avançada no módulo de Proteção em tempo real do sistema de arquivos pode resultar em maior utilização dos recursos (normalmente, somente arquivos recém-criados são verificados utilizando esses métodos). Recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Rastreamento do computador.

#### 4.1.1.6.1 Objetos

A seção **Objetos** permite definir quais componentes e arquivos do computador serão rastreados quanto a infiltrações.

**Memória operacional** - Rastreia procurando ameaças que atacam a memória operacional do sistema.

**Setores de inicialização** - Rastreia os setores de inicialização quanto à presença de vírus no registro de inicialização principal.

**Arquivos de email** - O programa oferece suporte às seguintes extensões: DBX (Outlook Express) e EML.

**Arquivos compactados** - O programa oferece suporte às seguintes extensões: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e muitas outras.

**Arquivos compactados de autoextração** - Os arquivos compactados de auto-extração (SFX, Self-extracting archives) são arquivos compactados que não requerem programas especializados - arquivos compactados - para se

descompactarem.

**Empacotadores em tempo real** - Depois da execução, os empacotadores em tempo real (ao contrário dos arquivos compactados padrão) fazem a descompactação na memória. Além dos empacotadores estáticos padrão (UPX, yoda, ASPack, FSG etc.), o scanner é compatível (graças à emulação do código) com muitos mais tipos de empacotadores.

#### 4.1.1.6.2 Opções

Na seção **Opções**, é possível selecionar os métodos a serem utilizados durante o rastreamento do sistema para verificar infiltrações. As opções disponíveis são:

**Heurística** - Uma heurística é um algoritmo que analisa a atividade (maliciosa) dos programas. A principal vantagem é a capacidade de identificar software malicioso que não existia ou que não era conhecido pelo banco de dados das assinaturas de vírus anterior. A desvantagem é uma probabilidade (muito pequena) de alarmes falsos.

**Heurística avançada/DNA/Assinaturas inteligentes** - A heurística avançada consiste em um algoritmo de heurística exclusivo desenvolvido pela ESET, otimizado para detecção de worms e cavalos de troia no computador e escrito em linguagens de programação de alto nível. Graças à heurística avançada, a capacidade de detecção do programa é significativamente superior. As assinaturas podem detectar e identificar vírus com segurança. Usando o sistema de atualização automática, novas assinaturas são disponibilizadas em poucas horas depois da descoberta da ameaça. A desvantagem das assinaturas é que elas detectam somente os vírus que conhecem (ou suas versões levemente modificadas).

Os **Aplicativos potencialmente indesejados** (PUAs) não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são:

- Novas janelas que você não via anteriormente (pop-ups, ads).
- Ativação e execução de processos ocultos.
- Uso aumentado de recursos do sistema.
- Alterações nos resultados de pesquisa.
- O aplicativo comunica-se com servidores remotos.

**Aplicativos potencialmente inseguros** - Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Ela inclui programas como ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário). Essa opção está desativada por padrão.

**ESET Live Grid** - Graças à tecnologia de reputação da ESET, as informações sobre os arquivos rastreados são verificadas em relação aos dados do ESET Live Grid baseado na nuvem , a fim de melhorar a detecção e a velocidade de rastreamento.

#### 4.1.1.6.3 Limpeza

As configurações de limpeza determinam o comportamento do scanner enquanto limpa os arquivos infectados. Há três níveis de limpeza:

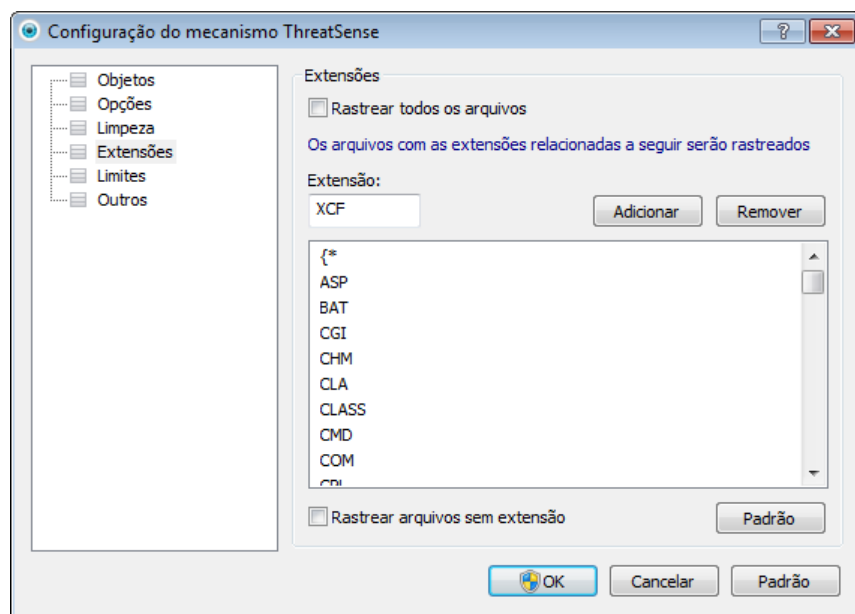
**Sem limpeza** - Os arquivos infectados não serão limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.

**Limpeza padrão** - O programa tentará limpar ou excluir automaticamente um arquivo infectado com base em uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma mensagem de informação localizada no canto inferior direito da tela. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá uma seleção de ações de acompanhamento. O mesmo ocorre quando uma ação predefinida não pode ser concluída.

**Limpeza rígida** - O programa limpará ou excluirá todos os arquivos infectados. As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, o usuário é solicitado a selecionar uma ação em uma janela de aviso.

**Aviso:** Se um arquivo compactado tiver um ou mais arquivos infectados, haverá duas opções para tratar o arquivo. No modo padrão (Limpeza padrão), o arquivo completo será excluído se todos os arquivos que ele contém forem arquivos infectados. No modo **Limpeza rígida**, o arquivo compactado seria excluído se tiver, pelo menos, um arquivo infectado, qualquer que seja o status dos outros arquivos no arquivo compactado.

#### 4.1.1.6.4 Extensão

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento. Se a opção **Rastrear todos os arquivos** estiver desmarcada, a lista será alterada para exibir todas as extensões de arquivos rastreados no momento.

Para habilitar o rastreamento de arquivos sem uma extensão, selecione a opção **Rastrear arquivos sem extensão**. A opção **Não rastrear arquivos sem extensão** é disponibilizada quando a opção **Rastrear todos os arquivos** é ativada.

A exclusão de arquivos será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa que está usando as extensões. Por exemplo, pode ser aconselhável excluir as extensões .edb, .eml e .tmp ao usar os servidores Microsoft Exchange.

Com os botões **Adicionar** e **Remover**, você pode autorizar ou proibir o rastreamento de extensões de arquivos específicas. Digitar uma **Extensão** ativa o botão **Adicionar**, que adiciona a nova extensão à lista. Selecione uma extensão na lista e, em seguida, clique no botão **Remover** para excluir essa extensão da lista.

Os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco substitui qualquer string de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter apenas os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista.

Para rastrear somente o conjunto padrão de extensões, clique no botão **Padrão** e clique em **Sim**, quando solicitado, para confirmar.

#### 4.1.1.6.5 Limites

A seção Limites permite especificar o tamanho máximo de objetos e nível de compactação de arquivos compactados a serem rastreados:

**Tamanho máximo do objeto** - Define o tamanho máximo de objetos a serem rastreados. O módulo antivírus determinado rastreará apenas objetos menores que o tamanho especificado. Essa opção apenas será alterada por usuários avançados que podem ter razões específicas para excluir objetos maiores do rastreamento. Valor padrão: sem limite.

**Tempo máximo do rastreamento para objecto (s)** - Define o valor de tempo máximo para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento. Valor padrão: sem limite.

**Nível de compactação de arquivos compactados** - Especifica a profundidade máxima do rastreamento de arquivos compactados. Valor padrão: 10.

**Tamanho máximo do arquivo no arquivo compactado** - Essa opção permite especificar o tamanho máximo de

arquivos para os arquivos contidos em arquivos compactados (quando são extraídos) a serem rastreados. Valor padrão: sem limite.

Se o rastreamento de um arquivo compactado for encerrado prematuramente por essa razão, o arquivo compactado permanecerá desmarcado.

**Observação:** Não recomendamos alterar os valores padrão; sob circunstâncias normais, não haverá razão para modificá-los.

#### 4.1.1.6.6 Outros

Na seção **Outros**, é possível configurar as seguintes opções:

**Registrar todos os objetos** - Se essa opção estiver selecionada, o arquivo de log mostrará todos os arquivos rastreados, mesmo os que não estiverem infectados. Por exemplo, se uma infiltração for encontrada dentro de um arquivo compactado, o log também listará os arquivos limpos contidos dentro do arquivo compactado.

**Ativar otimização inteligente** - Com a Otimização inteligente ativada, as configurações mais ideais são utilizadas para garantir o nível mais eficiente de rastreamento, mantendo simultaneamente a velocidade de rastreamento mais alta. Os diversos módulos de proteção fazem rastreamento de maneira inteligente, utilizando diferentes métodos de rastreamento e os aplicando a tipos específicos de arquivos. Se a Otimização inteligente estiver desativada, somente as configurações definidas pelo usuário no núcleo do ThreatSense do módulo particular serão aplicadas durante a realização de um rastreamento.

Ao configurar os parâmetros do mecanismo ThreatSense para um rastreamento do computador, as seguintes opções também estarão disponíveis:

**Rastrear fluxos dados alternativos (ADS)** - Fluxos de dados alternativos usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

**Executar rastreamento em segundo plano com baixa prioridade** - Cada sequência de rastreamento consome determinada quantidade de recursos do sistema. Se você estiver trabalhando com programas que exigem pesados recursos do sistema, você poderá ativar o rastreamento de baixa prioridade em segundo plano e economizar recursos para os aplicativos.

**Manter último registro de acesso** - Selecione essa opção para manter o tempo de acesso original dos arquivos rastreados, em vez de atualizá-lo (por exemplo, para uso com sistemas de backup de dados).

**Percorrer log de rastreamento** - Essa opção permite ativar/desativar o rolamento do log. Se selecionada, as informações rolam para cima dentro da janela de exibição.

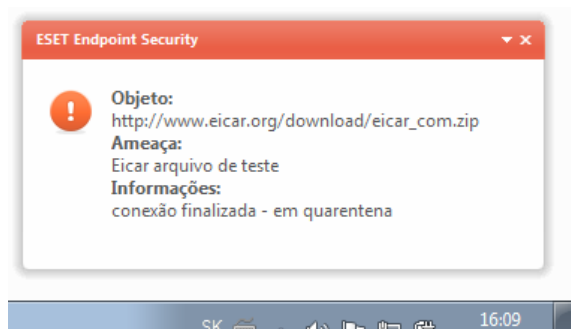
#### 4.1.1.7 Uma infiltração foi detectada

As ameaças podem alcançar o sistema a partir de vários pontos de entrada, tais como páginas da web, pastas compartilhadas, via email ou dispositivos removíveis (USB, discos externos, CDs, DVDs, disquetes, etc.).

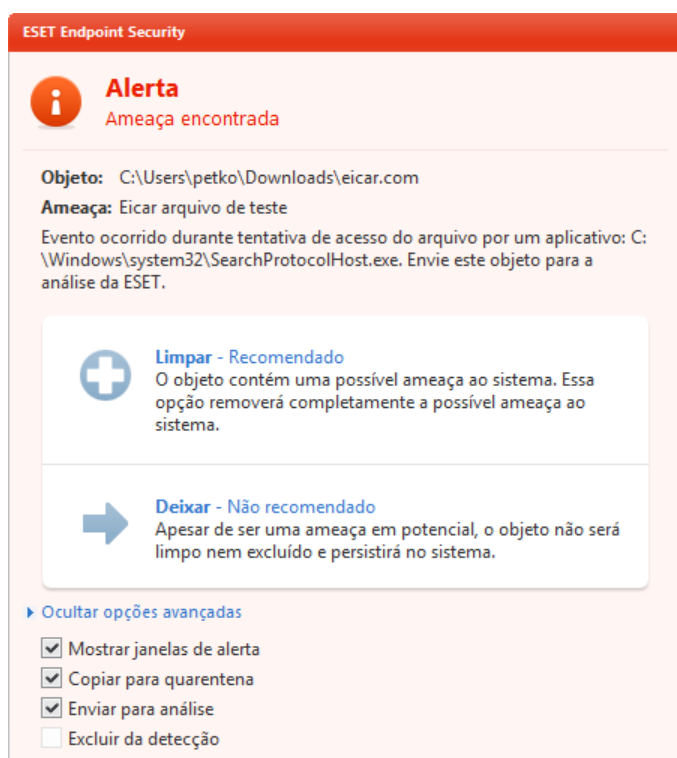
**Comportamento padrão**

Como um exemplo geral de como as infiltrações são tratadas pelo ESET Endpoint Security, as infiltrações podem ser detectadas usando

- Proteção em tempo real do sistema de arquivos,
- Proteção do acesso à web,
- Proteção do cliente de email ou
- Rastreamento sob demanda do computador,

Cada um usa o nível de limpeza padrão e tentará limpar o arquivo e movê-lo para a Quarentena ou encerrar a conexão. Uma janela de notificação é exibida na área de notificação, no canto inferior direito da tela. Para obter mais informações sobre níveis de limpeza e de comportamento, consulte Limpeza.

### Limpeza e exclusão

Se não houver uma ação predefinida a ser adotada para a Proteção em tempo real do sistema de arquivos, você será solicitado a selecionar uma opção em uma janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Nenhuma ação** estão disponíveis. Não se recomenda selecionar **Nenhuma ação**, pois os arquivos infectados não serão limpos. A exceção a isso é quando você tem certeza de que um arquivo é inofensivo e foi detectado por engano.

Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou um código malicioso a esse arquivo. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo para o seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Se um arquivo infectado estiver "bloqueado" ou em uso por um processo do sistema, ele somente será excluído após ter sido liberado (normalmente após a reinicialização do sistema).

### Exclusão de arquivos em arquivos compactados

No modo de limpeza Padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Tenha cautela ao executar um rastreamento com Limpeza rígida, com esse tipo de limpeza o arquivo compactado será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, etc., recomendamos que você faça o seguinte:

- Abra o ESET Endpoint Security e clique em Rastrear o computador.
- Clique em **Rastreamento inteligente** (para obter mais informações, consulte Rastreamento inteligente),
- Após a conclusão do rastreamento, revise o log para obter informações como o número de arquivos rastreados, infectados e limpos.

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

### 4.1.2 Mídia removível

O ESET Endpoint Security fornece rastreamento automático de mídia removível (CD/DVD/USB/...). Este módulo permite que você rastreie uma mídia inserida. Isso pode ser útil se a intenção do administrador do computador for evitar que os usuários usem uma mídia removível com conteúdo não solicitado.

**Ação a tomar após conectar dispositivos externos** - Selecione a ação padrão a ser executada quando um dispositivo de mídia removível for inserido no computador (CD/DVD/USB). Se a opção **Mostrar opções de rastreamento** for selecionada, será exibida uma notificação que lhe permite selecionar a ação desejada:

- **Rastrear agora** - Um rastreamento do computador sob demanda do dispositivo de mídia removível inserido será executado.
- **Rastrear mais tarde** - Nenhuma ação será executada e a janela **Novo dispositivo detectado** será fechada.
- **Configurar...** - Abre a seção de configuração da mídia removível.

ESET Endpoint Security
Novo dispositivo detectado
USB Storage (CORSAIR (F:\))
Rastrear agora
Rastrear depois
Configurar...
Sempre usar a opção selecionada

Além disso, o ESET Endpoint Security tem o recurso de Controle de dispositivos, que possibilita a definição de regras de utilização de dispositivos externos em um determinado computador. Acesse a seção Controle de dispositivos para obter mais detalhes sobre o controle de dispositivos.

### 4.1.3 Controle de dispositivos

O ESET Endpoint Security fornece controle automático de dispositivos (CD/DVD/USB/...). Esse módulo permite rastrear, bloquear ou ajustar filtros/permissões estendidos e seleciona como o usuário pode acessar e trabalhar com um determinado dispositivo. Isso pode ser útil se a intenção do administrador do computador for evitar o uso de dispositivos com conteúdo não solicitado pelos usuários.

**Dispositivos externos suportados**

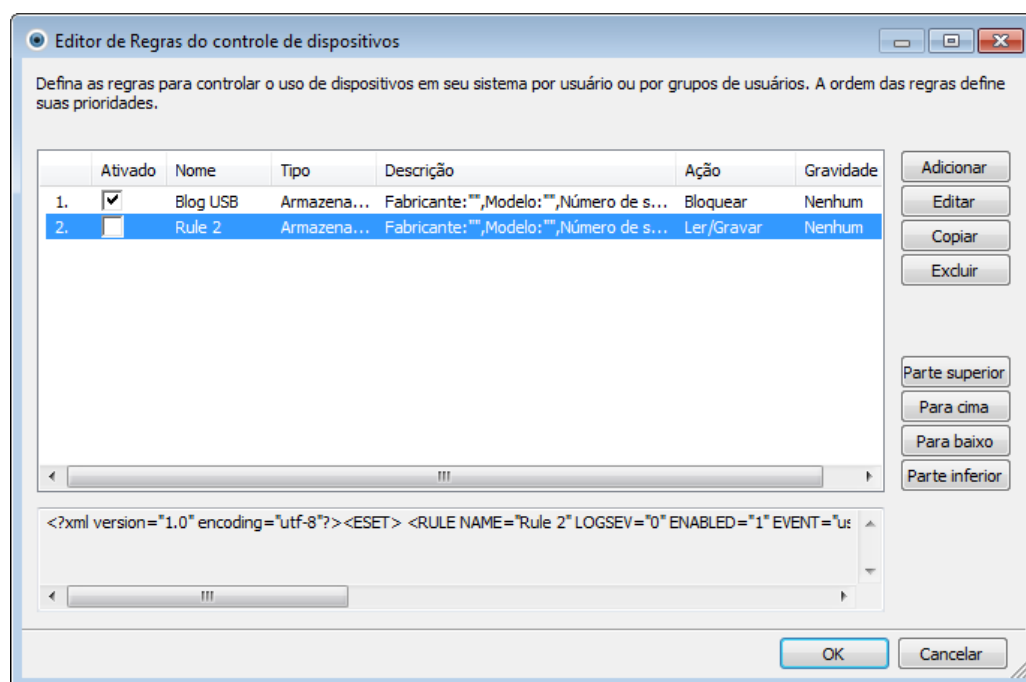
- CD/DVD/Blu-ray
- Armazenamento USB
- Dispositivo FireWire
- Dispositivo de imagens
- Impressora USB
- Bluetooth
- Leitor de cartão
- Modem
- Porta LPT/COM

As opções de configuração do Controle de dispositivos podem ser modificadas em **Configuração avançada** (F5) > **Controle de dispositivos**.

Marcar a caixa de seleção ao lado da opção **Integrar ao sistema** ativará o recurso de Controle de dispositivo no ESET Endpoint Security; você precisará reiniciar seu computador para que essa alteração seja implementada. Assim que o Controle de dispositivo for ativado, a opção **Configurar regras...** será ativada, permitindo que você abra a janela Editor de regras do controle de dispositivos.

Se o dispositivo externo inserido aplicar-se a uma regra existente que efetua a ação **Bloquear**, uma janela de notificação será exibida no canto inferior direito e o acesso ao dispositivo não será concedido.

### 4.1.3.1 Regras do controle de dispositivos

A janela **Editor de regras do controle de dispositivos** mostra as regras existentes e permite que se controle de forma precisa os dispositivos externos que os usuários conectam ao computador.

Determinados dispositivos podem ser permitidos ou bloqueados por usuário ou grupo de usuários e com base em parâmetros de dispositivos adicionais que podem ser especificados na configuração da regra. A lista de regras contém diversas descrições de uma regra, tais como nome, tipo de dispositivo externo, ação a ser realizada após conectar um dispositivo externo ao computador e a gravidade do relatório.

Clique em **Adicionar** ou **Editar** para gerenciar uma regra. Clique em **Copiar** para criar uma nova regra com as opções predefinidas usadas por outra regra selecionada. As cadeias XML exibidas ao clicar em uma regra podem ser copiadas para a área de transferência para ajudar os administradores do sistema a exportarem/importarem esses dados e usá-los, por exemplo no ESET Remote Administrator.

Ao pressionar CTRL e clicar, é possível selecionar mais de uma regra e aplicar as ações, tais como exclui-las ou movê-las para cima e para baixo na lista, em todas as regras selecionadas. A caixa de seleção **Ativado** desativará ou ativará uma regra; isso pode ser útil caso não deseje excluir uma regra permanentemente se você pretende usá-la no futuro.

O controle é realizado por regras classificadas na ordem que determina sua prioridade, com regras de prioridade mais alta na parte superior.

É possível clicar com o botão direito do mouse em uma regra para exibir o menu de contexto. Aqui, você pode definir o detalhamento de entradas de log (gravidade) de uma regra. As entradas de logs podem ser visualizadas a partir da janela principal do ESET Endpoint Security em **Ferramentas** > **Arquivos de log**.

### 4.1.3.2 Adição de regras do controle de dispositivos

Uma Regra de controle de dispositivos define a ação a ser tomada quando um dispositivo que corresponde aos critérios da regra é conectado ao computador.

Insira a descrição da regra no campo **Nome** para uma melhor identificação. Selecionar a caixa de seleção próxima a **Ativado** ativará ou desativará esta regra; isso pode ser útil caso não deseje excluir a regra permanentemente.

#### Tipo de dispositivo

Escolha o tipo de dispositivo externo no menu suspenso (USB/Bluetooth/FireWire/...). Os tipos de dispositivos são herdados do sistema operacional e podem ser visualizados no Gerenciador de dispositivos do sistema desde que um dispositivo esteja conectado ao computador. O tipo de dispositivo **Armazenamento óptico** no menu suspenso refere-se ao armazenamento de dados em uma mídia de leitura óptica (ex.: CDs e DVDs). Os dispositivos de armazenamento incluem discos externos ou leitores de cartão de memória convencionais conectados via USB ou FireWire. Scanners e câmeras são exemplos de dispositivos de imagens. Leitores de cartões inteligentes abrangem leitores de cartões inteligentes com um circuito integrado incorporado, como cartões SIM ou cartões de autenticação.

#### Direitos

O acesso a dispositivos que não sejam de armazenamento pode ser permitido ou bloqueado. Por outro lado, as regras de dispositivos de armazenamento permitem a seleção de um dos seguintes direitos:

- **Bloquear** - O acesso ao dispositivo será bloqueado.
- **Somente leitura** - Só será permitido ler o conteúdo do dispositivo.
- **Ler/Gravar** - Será permitido acesso total ao dispositivo.

Note que nem todos os direitos (ações) estão disponíveis para todos os tipos de dispositivos. Se um dispositivo tiver espaço de armazenamento, todas as três ações são disponibilizadas. Para dispositivos que não sejam de armazenamento, há apenas duas (por exemplo, a ação **Somente leitura** não está disponível para Bluetooth, o que significa que Bluetooth só pode ser permitido ou bloqueado).

Outros parâmetros que podem ser usados para ajustar as regras e adequá-las a dispositivos concretos. Todos os parâmetros não fazem diferenciação entre letras maiúsculas e minúsculas:

- **Fornecedor** - Filtragem por nome ou ID do fornecedor.
- **Modelo** - O nome específico do dispositivo.
- **Número de série** - Dispositivos externos geralmente têm seus próprios números de série. No caso de CD/DVD, este é o número de série da mídia em si, e não o da unidade de CD.

**Observação:** Se os três descritores acima estiverem vazios, a regra irá ignorar estes campos enquanto faz a correspondência.

**Dica:** A fim de descobrir os parâmetros de um dispositivo, crie uma regra de permissão para o tipo apropriado de dispositivos, conecte o dispositivo ao computador e, em seguida, verifique os detalhes no Log de controle de dispositivos.

As regras podem ser limitadas a determinados usuários ou grupos de usuários adicionando-os à **Lista de usuários**:

- **Adicionar** - Abre a janela de diálogo **Tipo de objeto: Usuários ou Grupos** que permite selecionar os usuários desejados.
- **Excluir** - Remove o usuário selecionado do filtro.

### 4.1.4 Sistema de prevenção de intrusos de host (HIPS)

O **Sistema de prevenção de intrusos de host** (HIPS) protege o sistema de malware ou de qualquer atividade que tentar prejudicar a segurança do computador. Ele utiliza a análise comportamental avançada em conjunto com as capacidades de detecção de filtro de rede para monitorar processos em execução, arquivos e chaves de registro. O HIPS é separado da proteção em tempo real do sistema de arquivos e não é um firewall; ele monitora somente processos em execução no sistema operacional.

O HIPS pode ser encontrado em **Configuração avançada** (F5) clicando em **Computador** > **HIPS**. O status do HIPS (ativado/desativado) é exibido na janela principal do ESET Endpoint Security, no painel **Configuração**, à direita da seção **Computador**.

As configurações do HIPS estão localizadas na **Configuração avançada** (F5). Para acessar o HIPS, na árvore Configuração avançada, clique em **Computador** > **HIPS**. O status do HIPS (ativado/desativado) é exibido na janela principal do ESET Endpoint Security, no painel **Configuração**, à direita da seção Computador.

**Aviso:** apenas um usuário experiente deve fazer alterações nas configurações do HIPS.

O ESET Endpoint Security tem uma tecnologia de Autodefesa incorporada que impede que o software malicioso danifique ou desabilite a proteção antivírus e anti-spyware. Dessa forma, você poderá ter certeza que seu sistema está protegido o tempo todo. As alterações executadas nas configurações **Ativar HIPS** e **Ativar autodefesa** entram em vigor depois que o sistema operacional Windows é reiniciado. A desativação de todo o sistema **HIPS** também exigirá uma reinicialização do computador.

A filtragem pode ser executada em um de quatro modos:

- **Modo automático com regras** - As operações são ativadas, exceto as regras predefinidas que protegem o sistema.
- **Modo interativo** - O sistema solicitará que o usuário confirme as operações.
- **Modo com base em políticas** - As operações são bloqueadas.
- **Modo de aprendizagem** - As operações são ativadas e uma regra é criada após cada operação. As regras criadas nesse modo podem ser visualizadas no **Editor de regras**, mas sua prioridade é menor que a prioridade das regras criadas manualmente ou das regras criadas no modo automático. Depois de selecionar **Modo de aprendizagem**, a opção**Notificar sobre a expiração do modo de aprendizagem em X dias** fica ativa. Ao término desse período, o modo de aprendizagem será desativado novamente. O prazo máximo é de 14 dias. Ao término desse período, uma janela pop-up será aberta e você poderá editar as regras e selecionar outro modo de filtragem.

O sistema HIPS monitora os eventos dentro do sistema operacional e reage a eles de acordo com regras similares às regras usadas no firewall pessoal. Clique em **Configurar regras...** para abrir a janela de gerenciamento de regras do HIPS. Aqui é possível selecionar, criar, editar ou excluir regras.

No exemplo a seguir demonstraremos como restringir o comportamento indesejado de aplicativos:

1. Nomeie a regra e selecione **Bloquear** no menu suspenso **Ação**.
2. Abra a guia **Aplicativos de destino**. Deixe a guia **Aplicativos de origem** em branco para que a nova regra seja aplicada a todos os aplicativos tentando realizar qualquer das operações verificadas na lista **Operações** nos aplicativos na lista **Nestes aplicativos**.
3. Selecione **Alterar estado de outro aplicativo** (todas as operações são descritas na seção Ajuda do produto, pressione a tecla F1 na janela identica à imagem a seguir).
4. Adicione um ou vários aplicativos que deseja proteger.
5. Ative a opção **Notificar usuário** para exibir uma notificação ao usuário sempre que a regra for aplicada.
6. Clique em **OK** para salvar a nova regra.

Editar regra

As regras definem como o Sistema de prevenção de intrusos de host decide quais aplicativos têm acesso permitido ou bloqueado a arquivos selecionados, a partes do registro ou a outros aplicativos. Também é possível deixar a escolha da ação para o usuário. Cada regra consiste em condições, que precisam ser atendidas, antes que uma regra seja aplicada e uma ação específica seja executada.

Configuração básica

Nome: Bloquear

Ação: Bloquear

Outras configurações

☑ Regra ativada

☑ Relatório

☑ Notificar usuário

Aplicativos de origem | Arquivos de destino | Aplicativos de destino | Registro de destino

Operações

☐ Debugging another application

☐ Intercept events from another application

☐ Terminate/suspend another application

☐ Start new application

☑ Modify state of another application

☐ Usar para todas as operações

Nestes aplicativos

C:\Windows\explorer.exe
C:\Windows\notepad.exe

Adicionar... | Adicionar grupo... | Editar... | Remover

OK | Cancelar

Uma janela de diálogo será exibida sempre que **Perguntar** for a ação padrão. Ela permite que o usuário escolha se deseja **Negar** ou **Permitir** a operação. Se o usuário não definir uma ação no tempo determinado, uma nova ação será selecionada com base nas regras.

ESET Endpoint Security

**Permitir esta operação?**

Sistema de prevenção de intrusos de host (HIPS)

**Aplicativo:** C:\Windows\explorer.exe

**Operação:** Iniciar novo aplicativo

**Alvo:** C:\Program Files\Internet Explorer\iexplore.exe

Permitir
O aplicativo será autorizado para prosseguir esta operação ou para executar esta ação.

Negar
O aplicativo não será autorizado para prosseguir esta operação ou para executar esta ação.

☐ Criar regra

☐ Lembrar temporariamente desta ação para este processo

Ocultar opções avançadas

☑ Criar uma regra válida apenas para este aplicativo

☑ Criar uma regra válida apenas para a operação

Iniciar novo aplicativo

☑ Criar uma regra válida apenas para o alvo

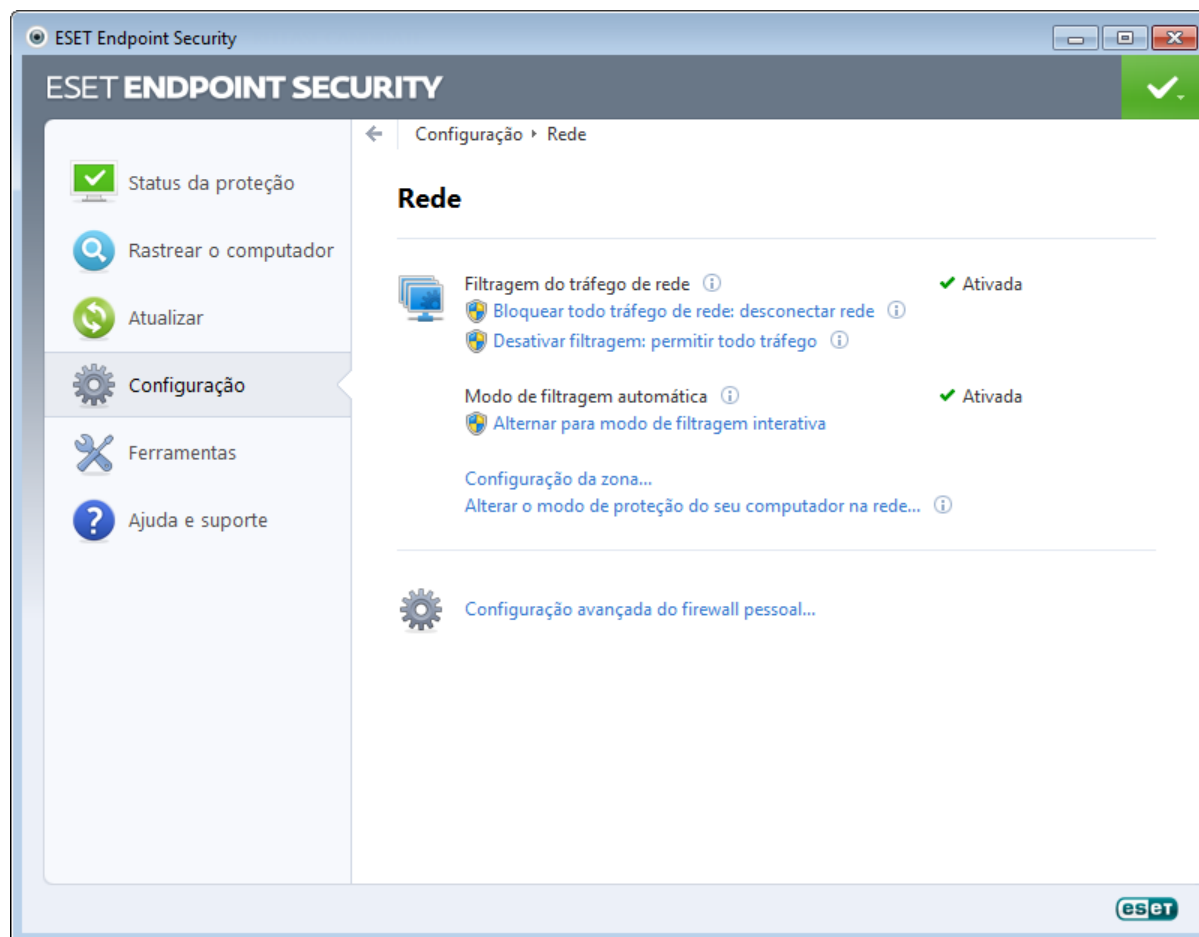
C:\Program Files\Internet Explorer\iexplore.exe

A janela da caixa de diálogo permite que você crie uma regra com base em qualquer nova ação que o HIPS detectar e então definirá as condições nas quais permitir ou negar essa ação. Os parâmetros exatos podem ser definidos depois de clicar em **Mostrar opções**. As regras criadas como esta são consideradas iguais às regras criadas manualmente, portanto a regra criada a partir de uma janela de diálogo pode ser menos específica que a regra que acionou a janela de diálogo. Isso significa que após a criação dessa regra, a mesma operação pode acionar a mesma janela.

A opção **Lembrar temporariamente desta ação para este processo** faz com que a ação (**Permitir** / **Negar**) seja utilizada até que ocorra uma alteração de regras ou o modo de filtragem seja ativado ou ocorra uma atualização do módulo do HIPS ou reinicialização do sistema. Depois de qualquer uma dessas três ações, as regras temporárias serão excluídas.

## 4.2 Rede

O firewall pessoal controla todo o tráfego de rede para e a partir do sistema. Isso é realizado através da permissão ou proibição de conexões individuais de rede, com base em regras de filtragem especificadas. Ele fornece proteção contra ataques de computadores remotos e ativa o bloqueio de alguns serviços. Ele também fornece proteção antivírus para protocolos HTTP, POP3 e IMAP. Esta funcionalidade representa um elemento muito importante na segurança do computador.

A configuração do firewall pessoal pode ser encontrada no painel **Configuração** depois de clicar em **Rede**. Aqui, é possível ajustar o modo de filtragem, regras e configurações detalhadas. Você também pode acessar mais configurações detalhadas do programa a partir daqui.

A única opção para bloquear todo o tráfego de rede é clicar em **Bloquear todo tráfego de rede: desconectar a rede**. Todas as comunicação de entrada e saída serão bloqueadas pelo firewall pessoal. Utilize essa opção somente se suspeitar de riscos de segurança críticos que requeiram a desconexão do sistema da rede.

A opção **Desativar filtragem: permitir todo tráfego** é o contrário do bloqueio de todo o tráfego de rede. Se ela for selecionada, todas as opções de filtragem do firewall pessoal serão desativadas, e todas as conexões de entrada e de saída serão permitidas. Ela tem o mesmo efeito como se nenhum firewall estivesse presente. Embora a Filtragem do tráfego de rede esteja no status de **Bloqueio**, a opção **Alternar para modo de filtragem** ativa o firewall.

As opções que se seguem estão disponíveis quando o Modo de filtragem automática é ativado:

- **Modo de filtragem automática** - Para alterar o modo de filtragem, clique na opção **Alternar para modo de filtragem automática**.
- **Configuração de zona...** - Exibe as opções de configuração da zona confiável.

Estas opções que se seguem estão disponíveis quando o Modo de filtragem interativa é ativado:

- **Modo de filtragem interativa** - Para alterar o modo de filtragem, clique em **Alternar para modo de filtragem automática** ou **Alternar para modo de filtragem automática com exceções** dependendo do modo de filtragem atual.
- **Configurar regras e zonas...** - Abre a janela **Configuração de zona e regra**, que permite definir como o firewall tratará a comunicação de rede.

**Alterar o modo de proteção do seu computador na rede...** - Permite escolher entre o modo de proteção restrito ou permitido.

**Configuração avançada de Firewall pessoal...** - Permite acessar as opções de configuração avançada do firewall.

### 4.2.1 Modos de filtragem

Cinco modos de filtragem estão disponíveis para o firewall pessoal do ESET Endpoint Security. Os modos de filtragem podem ser encontrados em **Configuração avançada** (F5) clicando em **Rede** > **Firewall pessoal**. O comportamento do firewall é alterado com base no modo selecionado. Os modos de filtragem também influenciam o nível de interação necessário do usuário.

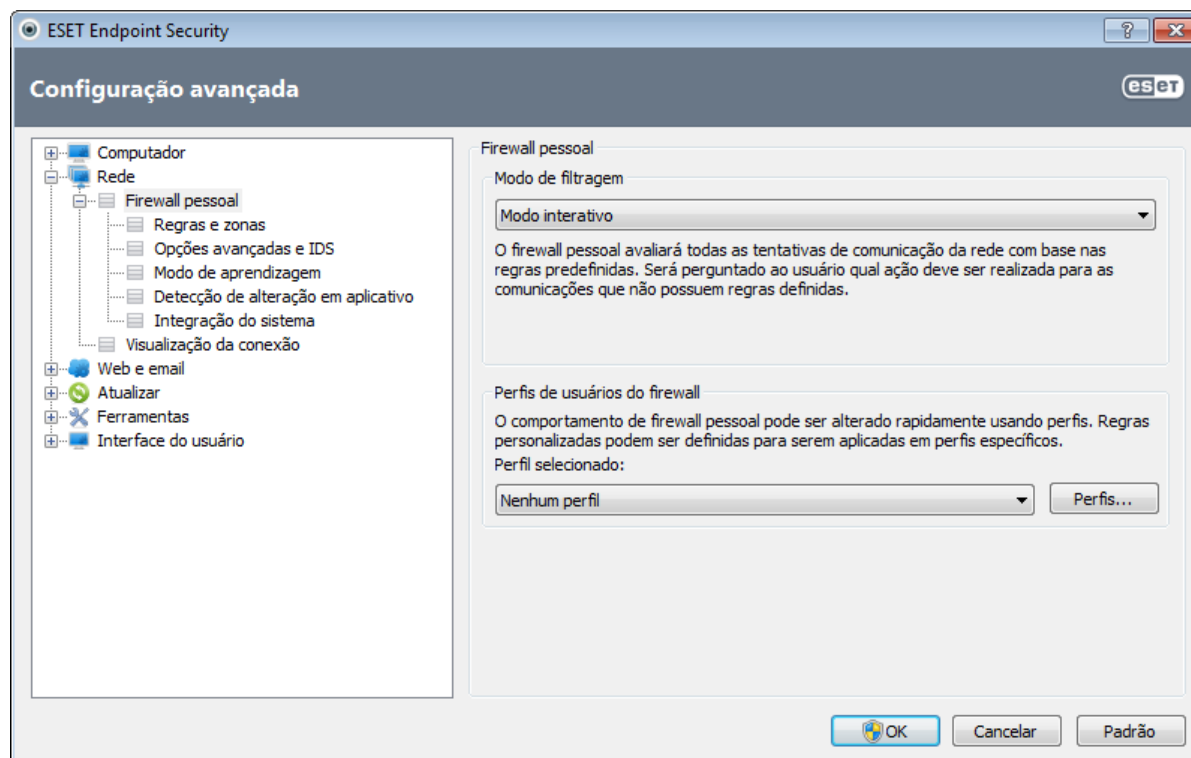
A filtragem pode ser executada em um de cinco modos:

**Modo automático** - O modo padrão. Esse modo é adequado para usuários que preferem o uso fácil e conveniente do firewall sem nenhuma necessidade de definir regras. O modo automático permite todo tráfego de entrada para o sistema e bloqueia todas as novas conexões iniciadas a partir do lado da rede.

**Modo automático com exceções (regras definidas pelo usuário)** - Além do modo automático, também é possível adicionar regras personalizadas definidas pelo usuário.

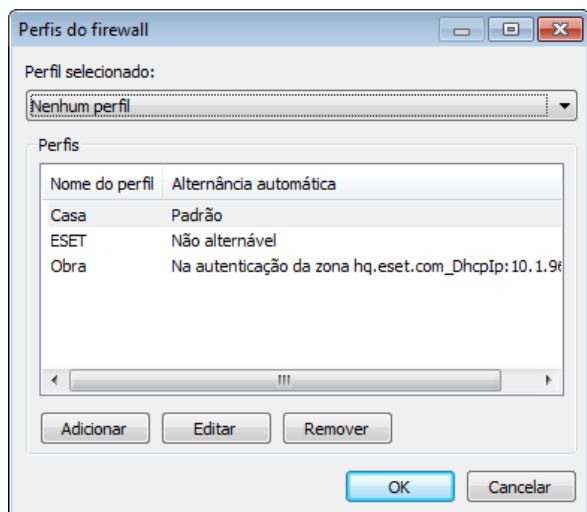
**Modo interativo** - Permite que você crie uma configuração personalizada para seu firewall pessoal. Quando uma comunicação para a qual não há regras aplicadas for detectada, será exibida uma janela de diálogo com a informação de uma conexão desconhecida. A janela de diálogo dá a opção de permitir ou negar a comunicação, e a decisão de permitir ou negar pode ser lembrada como uma nova regra para o firewall pessoal. Se o usuário escolher criar uma nova regra neste momento, todas as futuras conexões desse tipo serão permitidas ou bloqueadas de acordo com a regra.

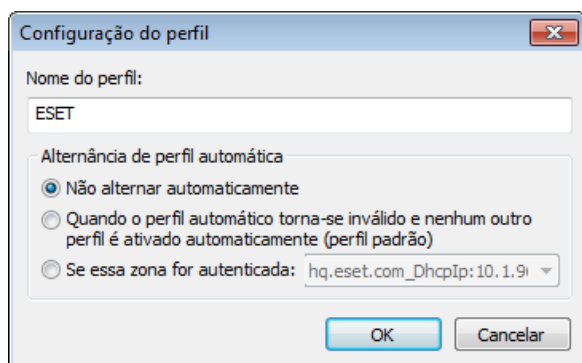
**Modo com base em políticas** - Bloqueia todas as conexões que não são definidas por uma regra específica que as permite. Esse modo permite que os usuários avançados definam as regras que permitem apenas as conexões desejadas e seguras. Todas as outras conexões não especificadas serão bloqueadas pelo firewall pessoal.

**Modo de aprendizagem** - Cria e salva automaticamente as regras e é adequado para a configuração inicial do firewall pessoal. Nenhuma interação com o usuário é exigida, porque o ESET Endpoint Security salva as regras de acordo com os parâmetros predefinidos. O modo de aprendizagem não é seguro e deve ser apenas usado até que todas as regras para as comunicações exigidas tenham sido criadas.

Os Perfis são uma ferramenta para controlar o comportamento do firewall pessoal do ESET Endpoint Security.

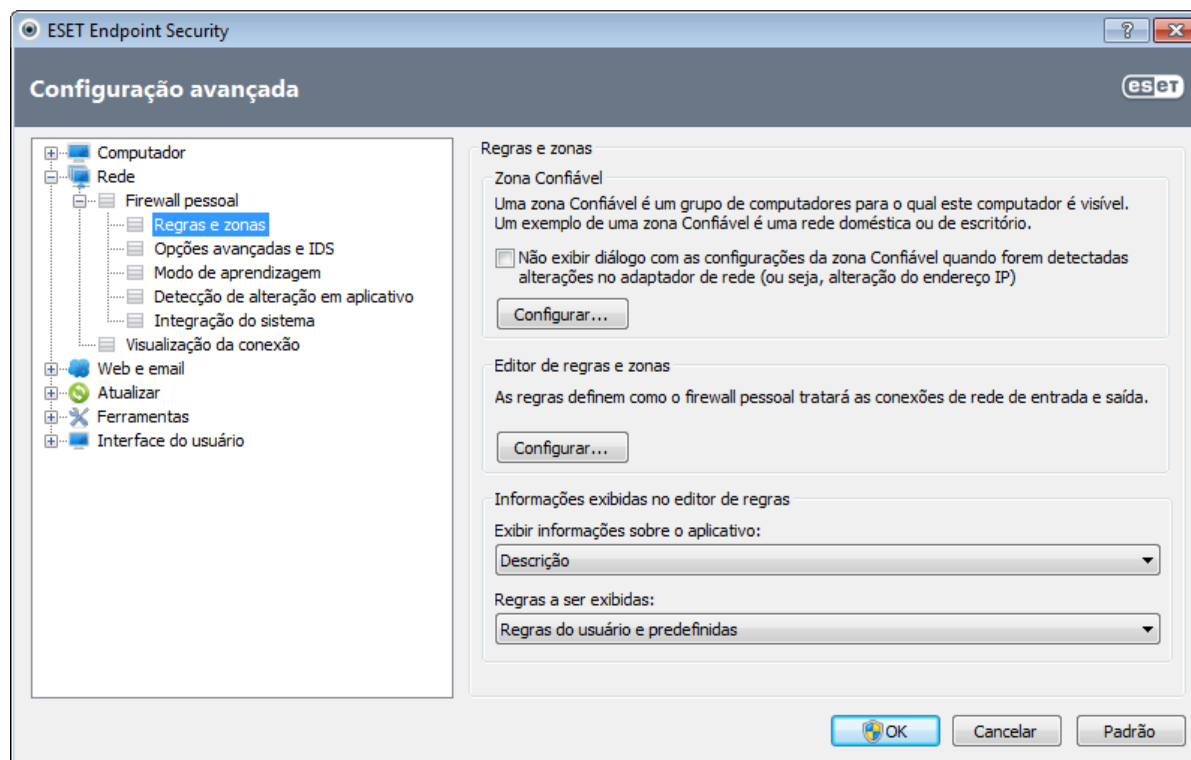
### 4.2.2 Perfis do firewall

Os perfis podem ser usados para controlar o comportamento do firewall pessoal do ESET Endpoint Security. Ao criar ou editar uma regra de firewall pessoal, você pode atribuí-la a um perfil específico ou aplicá-la a cada perfil. Quando você seleciona um perfil, apenas as regras globais (regras sem nenhum perfil especificado) e as regras que foram atribuídas a esse perfil são aplicadas. Você pode criar vários perfis com regras diferentes atribuídas para alterar com facilidade o comportamento do firewall pessoal.

Clique no botão **Perfis...** (veja a figura na seção Modos de filtragem) para abrir a janela **Perfis do firewall**, onde você pode **Adicionar**, **Editar** ou **Remover** perfis. Observe que para **Editar** ou **Remover** um perfil, ele não pode estar selecionado no menu suspenso **Perfil selecionado**. Ao adicionar ou editar um perfil, você pode também definir as condições que o acionam.

Ao criar um perfil, você pode selecionar eventos que acionarão o perfil. As opções disponíveis são:

- **Não alternar automaticamente** - O acionador automático está desativado (o perfil deve ser ativado manualmente).
- **Quando o perfil automático torna-se inválido e nenhum outro perfil é ativado automaticamente (perfil padrão)** - Quando o perfil automático torna-se inválido (se o computador estiver conectado a uma rede não confiável (consulte a seção Autenticação de rede) e nenhum outro perfil for ativado em seu lugar (o computador não estiver conectado a outra rede confiável), o firewall pessoal alternará para esse perfil. Apenas um perfil pode usar esse acionador.
- **Se essa zona for autenticada** - Esse perfil será acionado quando a zona especificada for autenticada (consulte a seção Autenticação de rede).

Quando o firewall pessoal alternar para outro perfil, uma notificação será exibida no canto inferior direito próximo ao relógio do sistema.

### 4.2.3 Configuração e uso de regras

As regras representam um conjunto de condições utilizadas para testar significativamente todas as conexões de rede e todas as ações atribuídas a essas condições. Com o firewall pessoal, é possível definir a ação a ser tomada se uma conexão definida por uma regra for estabelecida. Para acessar a configuração de filtragem de regras, navegue até **Configuração avançada** (F5) > **Rede** > **Firewall pessoal** > **Regras e zonas**.

Clique em **Configuração...** na seção **Zona confiável** para exibir a janela de configuração da zona confiável. A opção **Não exibir com as configurações da zona confiável...** permite ao usuário desativar a janela de configuração da zona confiável toda vez que a presença de uma nova sub-rede for detectada. A configuração da zona especificada atualmente é automaticamente usada.

**OBSERVAÇÃO:** Se o firewall pessoal estiver configurado como **Modo automático**, algumas configurações não estarão disponíveis.

Clique no botão Configuração... na seção **Editor de regras e zonas** para exibir a janela **Configuração de zona e regra**, onde uma visão geral das regras ou zonas é exibida (com base na guia selecionada no momento). A janela é dividida em duas seções. A seção superior lista todas as regras em uma exibição reduzida. A seção inferior exibe detalhes sobre a regra selecionada no momento, na seção superior. A parte inferior da janela possui os botões **Novo**, **Editar** e **Excluir (Del)**, que permitem configurar as regras.

As conexões podem ser divididas em conexões de entrada e de saída. As conexões de entrada são iniciadas por um computador remoto que tenta estabelecer uma conexão com o sistema local. As conexões de saída funcionam de maneira oposta - o sistema local contata um computador remoto.

Se uma nova comunicação desconhecida for detectada, é preciso considerar cuidadosamente se vai permiti-la ou negá-la. As conexões não solicitadas, não seguras ou desconhecidas representam um risco de segurança para o sistema. Se tal conexão for estabelecida, recomenda-se que seja dada atenção especial ao computador remoto e ao aplicativo tentando conectar-se ao computador. Muitas ameaças tentam obter e enviar dados particulares ou fazem download de outros aplicativos maliciosos para o computador/sistema local. O firewall pessoal permite que o usuário detecte e finalize tais conexões.

**Exibir informações sobre o aplicativo** permite definir como os aplicativos serão exibidos na lista de regras. As opções disponíveis são:

- **Caminho completo** - Caminho completo para o executável do aplicativo.
- **Descrição** - Descrição do aplicativo.
- **Nome** - Nome do executável do aplicativo.

Selecione que tipo de regras será exibido na lista **Regras a serem exibidas**:

- **Somente regras definidas pelo usuário** - Exibe somente as regras criadas pelo usuário.
- **Regras do usuário e predefinidas** - Exibe todas as regras definidas pelo usuário e as regras predefinidas.
- **Todas as regras (incluindo o sistema)** - Todas as regras são exibidas.

#### 4.2.3.1 Configuração de regras

A configuração de regras permite que você visualize todas as regras aplicadas ao tráfego gerado por aplicativos individuais nas zonas confiáveis e na Internet. Por padrão, as regras são adicionadas automaticamente, de acordo com as opções informadas pelo usuário para uma nova comunicação. Para ver mais informações sobre um aplicativo na parte inferior dessa janela, clique no nome do aplicativo.

Configuração de zona e regra

Regras | Zonas

A&s regras definem como o firewall tratará a comunicação de rede. As regras podem permitir ou negar a comunicação de determinados aplicativos, computadores remotos e portas específicas. Para obter mais informações sobre as regras, clique aqui.

Alternar exibição detalhada de todas as regras — Exibir regras usadas no perfil: Tudo

| Aplicativo/Regra | Entrada de zon... | Saída de zona ... | Entrada de Int... | Saída de Int... |
|---|---|---|---|---|
| Bloquear solicitações de entrada RPC | | | Negar | |
| Permitir a saída de mensagens IGMP | | | | |
| Permitir a entrada de mensagens IGMP a p... | | | | |
| Host Process for Windows Services | Específico | Específico | Específico | Específico |
| Windows Logon User Interface Host | Específico | Específico | Específico | Específico |
| Services and Controller app | Específico | Específico | Específico | Específico |
| Local Security Authority Process | Permitir | Específico | Permitir | Específico |
| Windows Logon Application | Permitir | Específico | Permitir | Específico |
| System | Específico | Específico | Específico | Específico |
| Microsoft Outlook | Permitir | Específico | Permitir | Específico |

**Descrição do arquivo:** Windows Logon User Interface Host
**Empresa:** Microsoft Corporation
**Versão do arquivo:** 6.1.7601.17514 (win7sp1_rtm.101119-1850)
**Nome original:** logonui.exe
**Copyright:** © Microsoft Corporation. All rights reserved.

Novo | Editar | Excluir (Del)

OK | Cancelar

No início de cada linha correspondente a uma regra, há um botão que permite ampliar/recolher (+/-) as informações. Clique no nome do aplicativo na coluna **Aplicativo/Regra** para exibir informações sobre a regra na parte inferior dessa janela. Você pode usar o menu de contexto para alterar o modo de exibição. O menu de contexto também pode ser usado para adicionar, editar e excluir regras.

**Zona confiável (entrada/saída)** - Ações relacionadas às comunicações de entrada e saída na zona confiável.

**Internet (entrada/saída)** - Ações relacionadas à conexão com a Internet para comunicações de entrada e saída.

Para cada tipo (direção) de comunicação, você pode selecionar as seguintes ações:

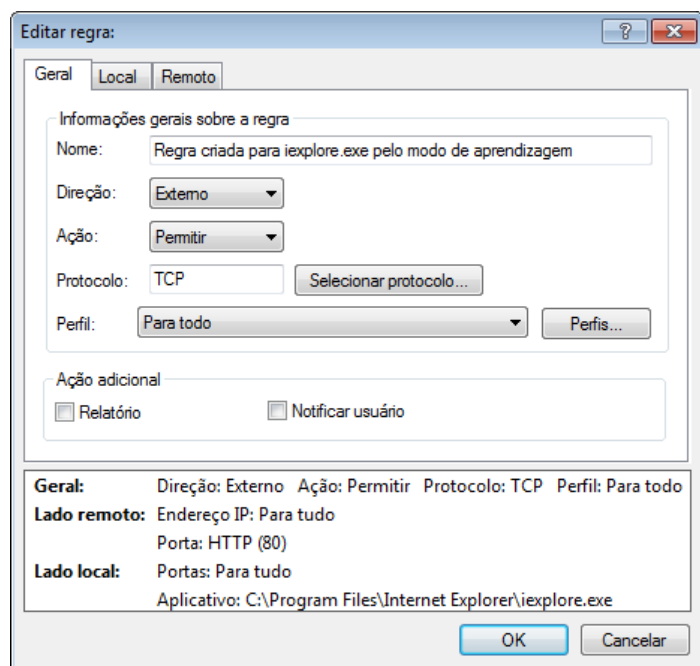
- ✔ **Permitir** - Para permitir a comunicação.
- ? **Perguntar** – Será solicitada sua permissão ou proibição sempre que uma comunicação for estabelecida.
- ✖ **Negar** - Para negar uma comunicação.
- ☰ **Específico** - Não é possível classificar com relação às outras ações. Por exemplo, se um endereço IP ou porta são permitidos por meio do firewall pessoal, ele não pode ser classificado com certeza, se as comunicações de entrada ou saída de um aplicativo relacionado forem permitidas.

Ao instalar um novo aplicativo que acessa a rede ou se houver uma modificação em uma conexão existente (endereço remoto, número de porta, etc.), uma nova regra deve ser criada. Para editar uma regra existente, verifique se a guia **Regras** está selecionada e clique no botão **Editar**.

#### 4.2.3.2 Edição de regras

A modificação é necessária toda vez que qualquer um dos parâmetros monitorados é alterado. Nesse caso, a regra não preenche completamente as condições e a ação especificada não pode ser aplicada. Se os parâmetros foram alterados, a conexão pode ser recusada, o que pode resultar em problemas com a operação do aplicativo em questão. Um exemplo é uma alteração do endereço de rede ou do número de porta para o local/endereço remoto.

A parte superior da janela contém três guias:

- **Geral** - Especifica um nome de regra, a direção da conexão, a ação, o protocolo e o perfil ao qual a regra se aplicará.
- **Local** - Exibe informações sobre o lado local da conexão, incluindo o número da porta local ou o intervalo de portas e o nome do aplicativo de comunicação.
- **Remoto** - Esta guia contém informações sobre a porta remota (intervalo de portas). Ela também permite que o usuário defina uma lista de endereços IP remotos ou zonas para uma determinada regra.

**Protocolo** representa o protocolo de transferência usado para a regra. Clique em **Selecionar protocolo...** para abrir a janela Seleção de protocolo.

Por padrão, todas as regras estão ativadas **Para todos** os perfis. Alternativamente, selecione um perfil de firewall personalizado usando o botão **Perfis...**.

Se você clicar em **Registrar**, a atividade conectada com a regra será registrada em um log. A opção **Notificar usuário** exibe uma notificação quando a regra é aplicada.

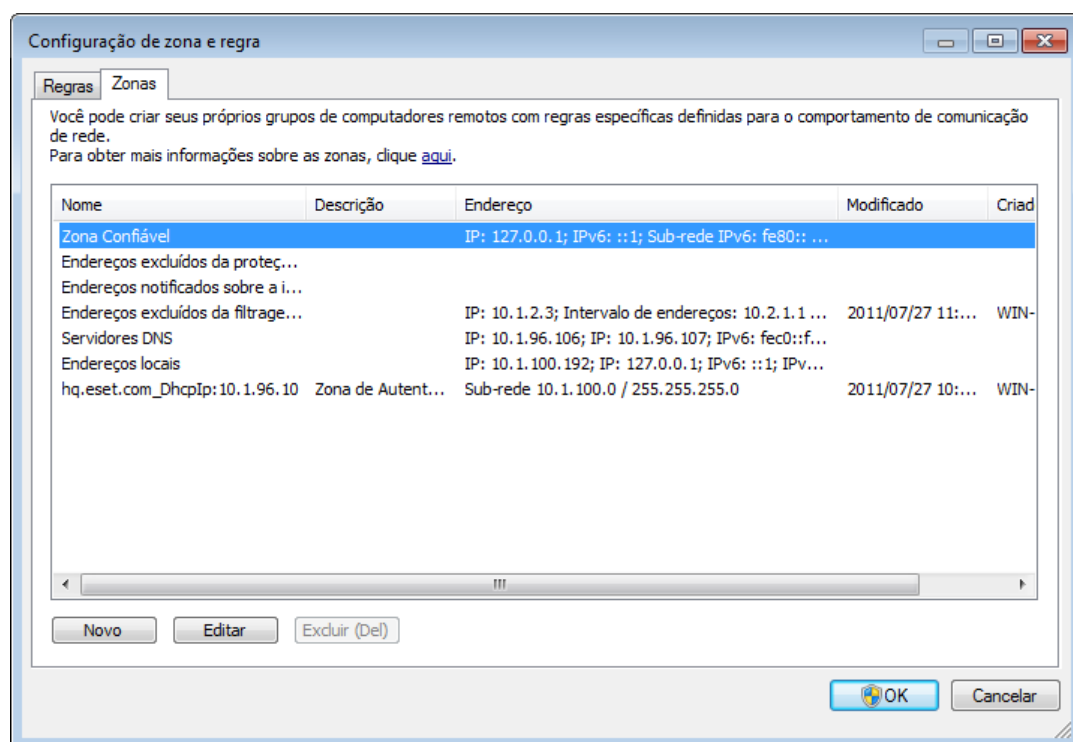
A caixa de informações exibe um resumo da regra na parte inferior das três guias. Você verá as mesmas informações se clicar na regra na janela principal (**Ferramentas** > **Conexões de rede**; clique com o botão direito do mouse na regra e ative a opção **Mostrar detalhes** (consulte o capítulo Conexões de rede)).

Ao criar uma nova regra, é preciso digitar o nome da regra no campo **Nome**. Selecione a direção para a qual a regra se aplica no menu suspenso **Direção**. Defina a ação a ser executada quando um canal de comunicação encontra a regra no menu suspenso **Ação**.

Um bom exemplo de adição de uma nova regra é permitir que o seu navegador da Internet acesse a rede. Os itens a seguir devem ser fornecidos neste caso:

- Na guia **Geral**, ative a comunicação de saída por meio dos protocolos TCP e DP.
- Adicione o processo que representa o aplicativo do seu navegador (para o Internet Explorer, é iexplore.exe) na guia **Local**.
- Na guia **Remoto**, ative a porta número 80 somente se você deseja permitir atividades de navegação padrão na Internet.

### 4.2.4 Configuração de zonas

Na janela **Configuração de zona**, você pode especificar o nome da zona, a descrição, a lista de endereços de rede e a autenticação da zona (consulte Autenticação de zona - Configuração de cliente).

A zona representa um grupo de endereços de rede que cria um grupo lógico. A cada endereço no grupo são atribuídas regras semelhantes definidas centralmente para todo o grupo. Um exemplo de tal grupo é a **Zona confiável**. A Zona confiável representa um grupo de endereços de rede que são de total confiança e que não são bloqueados pelo firewall pessoal de maneira alguma.

Essas zonas podem ser configuradas utilizando a guia **Zonas** na janela **Configuração de zona e regra**, clicando no botão **Editar**. Insira um **Nome** para a zona e uma **Descrição**, depois adicione um endereço IP remoto clicando no botão **Adicionar endereço IPv4/IPv6**.

#### 4.2.4.1 Autenticação de rede

Para os computadores móveis, é recomendável verificar a credibilidade da rede à qual você está se conectando. A Zona confiável é identificada pelo endereço IP local do adaptador de rede. Os computadores móveis geralmente inserem redes com endereços IP semelhantes à rede confiável. Se as configurações da Zona confiável não forem alternadas manualmente para **Proteção rígida**, o firewall pessoal continuará a usar o modo **Permitir compartilhamento**.

Para evitar esse tipo de situação, recomendamos o uso da autenticação de zona.

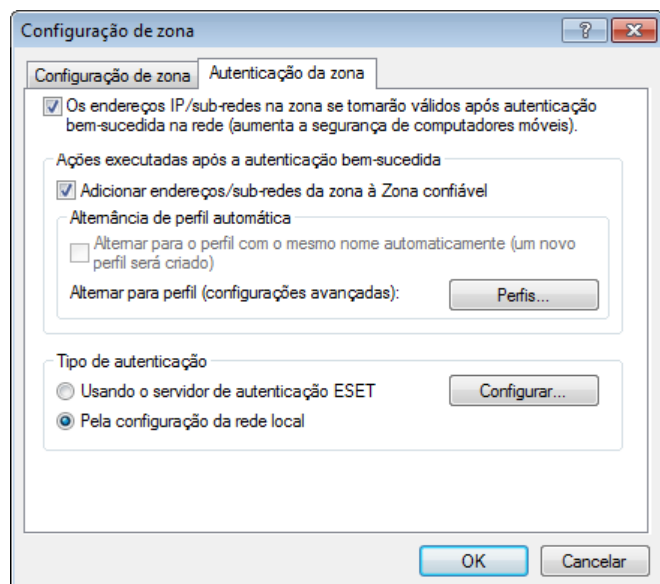
##### 4.2.4.1.1 Autenticação de zona - Configuração de cliente

Na janela **Configuração de zona e regra**, clique na guia **Zonas** e crie uma nova zona usando o nome da zona autenticada pelo servidor. Em seguida, clique em **Adicionar endereço IPv4** e selecione a opção **Sub-rede** para adicionar uma máscara de sub-rede que contenha o servidor de autenticação.

Clique na guia **Autenticação de zona**. Cada zona pode ser definida para autenticar ao servidor. A zona (seu endereço IP e sub-rede) será válida depois que sua autenticação ocorrer com êxito, ou seja, ações como alternar para um perfil de firewall e adicionar um endereço/sub-rede da zona à Zona confiável só serão executadas depois que a autenticação tiver sido concluída com sucesso.

Selecione a opção **Os endereços IP/sub-redes na zona se tornarão válidos ...** para criar uma zona. Ela se tornará inválida se a autenticação for malsucedida. Para selecionar um perfil de firewall pessoal a ser ativado após uma autenticação bem-sucedida da zona, clique no botão **Perfis...**.

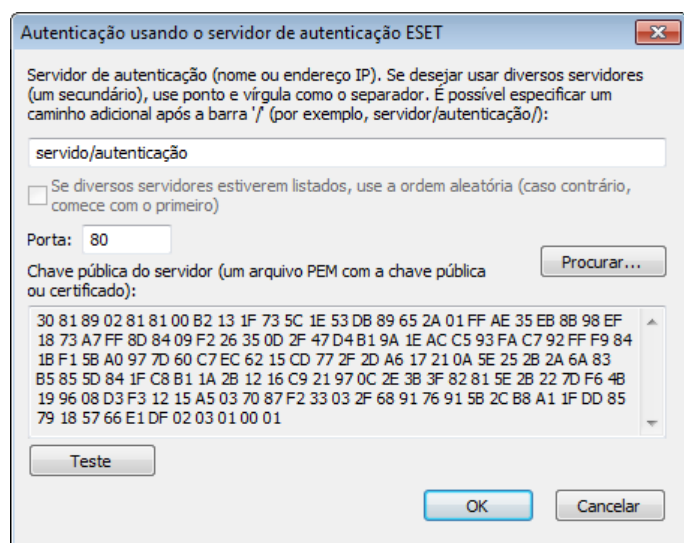
Se você selecionar a opção **Adicionar endereços/sub-redes da zona à Zona confiável**, os endereços/sub-redes da zona serão adicionados à Zona confiável após a autenticação bem-sucedida (recomendado). Se a autenticação for malsucedida, os endereços não serão adicionados à Zona confiável. Se a opção **Alternar para o perfil com o mesmo nome automaticamente (um novo perfil será criado)** estiver ativa, o novo perfil será criado após a autenticação

bem-sucedida. Clique no botão **Perfis...** para abrir a janela Perfi do firewall.

Há dois tipos de autenticação disponíveis:

**1) Usando o servidor de autenticação da ESET**

A autenticação de zona procura por um servidor específico na rede e usa uma criptografia assimétrica (RSA) para autenticar o servidor. O processo de autenticação é repetido para cada rede à qual o computador se conecta. Clique em **Configuração...** e especifique um nome de servidor, uma porta de escuta do servidor e uma chave pública que corresponda à chave privada do servidor (consulte a seção Autenticação de zona - Configuração de servidor). O nome do servidor pode ser inserido na forma de um endereço IP, um DNS ou um nome NetBios. O nome do servidor pode ser seguido por um caminho especificando o local da chave no servidor (por exemplo, nome-do-servidor_/diretório1/diretório2/autenticação). Insira vários servidores, separados por ponto e vírgulas, para atuar como servidores alternativos se o primeiro não estiver disponível.

A chave pública pode ser um arquivo de um dos seguintes tipos:

- Chave pública PEM codificada (.pem)
  Essa chave pode ser gerada usando o servidor de autenticação ESET (consulte a seção Autenticação de zona - Configuração de servidor).
- Chave pública codificada
- Certificado de chave pública (.crt)

Para testar suas configurações, clique no botão **Testar**. Se a autenticação for bem-sucedida, será exibida uma mensagem de Autenticação bem-sucedida do servidor. Se a autenticação não estiver configurada corretamente, será exibida uma das seguintes mensagens de erro:

Falha na autenticação do servidor. Tempo máximo para autenticação decorrido.
O servidor de autenticação está inacessível. Verifique o nome do servidor/endereço IP e/ou verifique as configurações

do firewall pessoal das seções do cliente e do servidor.

Ocorreu um erro ao comunicar com o servidor.
O servidor de autenticação não está em execução. Inicie o serviço do servidor de autenticação (consulte a seção Autenticação de zona - Configuração de servidor).

O nome da zona de autenticação não corresponde à zona do servidor.
O nome da zona configurada não corresponde à zona do servidor de autenticação. Revise as duas zonas e certifique-se de que seus nomes sejam idênticos.

Falha na autenticação do servidor. O endereço do servidor não foi encontrado na lista de endereços da zona determinada.
O endereço IP do computador executando o servidor de autenticação está fora do intervalo de endereços IP definido da configuração atual da zona.

Falha na autenticação do servidor. Provavelmente uma chave pública inválida foi inserida.
Verifique se a chave pública especificada corresponde à chave privada do servidor. Verifique também se o arquivo de chave pública não está corrompido.

**2) Pela configuração da rede local**

A autenticação é executada com base nos parâmetros do adaptador da rede local. A zona será autenticada se todos os parâmetros selecionados da conexão ativa forem válidos.

Autenticação pela configuração da rede local
A autenticação será bem-sucedida se todas as condições selecionadas para a conexão ativa forem cumpridas. Ambos os endereços IPv4 e IPv6 são permitidos. Vários endereços estão separados por um ponto e vírgula.
Configuração do adaptador para atender
Local Area Connection
Preencher com configurações de conexão selecionadas
Configurações gerais do adaptador
Quando o sufixo DNS atual for (exemplo: "empresa.com"):
hq.eset.com
Quando o endereço IP do servidor WINS for:
Quando o endereço IP do servidor DNS for:
10.1.96.106;10.1.96.107
Quando o endereço IP local for:
10.1.100.192;fe80::2429:5962:b6:6257
Quando o endereço IP do servidor DHCP for:
10.1.96.10
Quando o endereço IP do gateway for:
10.1.100.1
Tipo adaptor de rede:
Adaptador virtual (VPN, túnel...)
Adaptador de rede físico
Configurações de conexão sem fio
Quando o SSID sem fio for:
Quando o perfil da conexão for:
Quando a conexão estiver segura
Configurações gerais para todos os adaptadores (aplicáveis para vários adaptadores de rede)
Apenas uma conexão ativa
Nenhuma conexão sem fio estabelecida
Nenhuma conexão insegura sem fio estabelecida
OK
Cancelar

### 4.2.4.1.2 Autenticação de zona - Configuração de servidor

O processo de autenticação pode ser executado por qualquer computador/servidor conectado à rede que deva ser autenticado. O aplicativo Servidor de autenticação ESET precisa estar instalado em um computador/servidor que esteja sempre acessível para autenticação quando um cliente tentar se conectar à rede. O arquivo de instalação do aplicativo Servidor de autenticação ESET está disponível para download no site da ESET.

Depois de instalar o aplicativo Servidor de autenticação ESET, uma janela de diálogo será exibida (você pode acessar o aplicativo clicando em **Iniciar** > **Programas** > **ESET** > **Servidor de autenticação ESET**).

Para configurar o servidor de autenticação, insira o nome da zona de autenticação, a porta de escuta do servidor (o padrão é 80), bem como o local para armazenar o par de chaves pública e privada. Em seguida, gere as chaves pública e privada que serão utilizadas no processo de autenticação. A chave privada permanecerá no servidor, enquanto a chave pública precisará ser importada no lado do cliente na seção de autenticação da zona, ao definir uma zona na configuração do firewall.

### 4.2.5 Estabelecimento de uma conexão - detecção

O firewall pessoal detecta cada conexão de rede recém-criada. O modo de firewall ativo determina quais ações serão executadas para a nova regra. Se o **Modo automático** ou o **Modo com base em políticas** estiver ativado, o firewall pessoal executará ações predefinidas sem nenhuma interação com o usuário. O modo interativo exibe uma janela de informações que reporta a detecção de uma nova conexão de rede, suplementada com informações detalhadas sobre a conexão. O usuário pode escolher permitir a conexão ou recusá-la (bloqueio). Se houver necessidade de permitir várias vezes a mesma conexão na janela de diálogo, recomendamos que você crie uma nova regra para a conexão. Para isso, selecione a opção **Lembrar ação (criar regra)** e salve a ação como uma nova regra para o firewall pessoal. Se o firewall reconhecer a mesma conexão no futuro, ele aplicará a regra existente sem solicitar a interação do usuário.

ESET Endpoint Security

Tráfego de entrada

Zona Confiável

Um computador remoto da zona Confiável está tentando se comunicar com um aplicativo em execução neste computador. Deseja permitir esta comunicação?

**Aplicativo:** FileZilla Server
**Editor:** Desconhecido
**Computador remoto:** 10.0.2.2
**Porta local:** 21 (ftp)

Permitir
A comunicação com um computador remoto será permitida para o aplicativo selecionado.

Negar
A comunicação com um computador remoto será negada para o aplicativo selecionado.

Lembrar ação (criar regra)
Lembrar temporariamente ação para o processo

Mostrar opções avançadas

Tenha cuidado ao criar novas regras e permita apenas as conexões seguras. Se todas as conexões forem permitidas, então o firewall pessoal falhará em realizar seu propósito. Estes são os parâmetros importantes para as conexões:

- **Lado remoto** - Somente permita conexões para endereços confiáveis e conhecidos.
- **Aplicativo local** - Não é aconselhável permitir conexões para aplicativos e processos desconhecidos.
- **Número da porta** - Em circunstâncias normais, a comunicação em portas comuns (como, por exemplo, o tráfego da web - porta 80) deve ser permitida.

Para se proliferar, as ameaças de computador usam frequentemente a Internet e conexões ocultas para ajudar a infectar sistemas remotos. Se as regras forem configuradas corretamente, um firewall pessoal se tornará uma ferramenta útil para a proteção contra diversos ataques de códigos maliciosos.

### 4.2.6 Registro em log

O firewall pessoal do ESET Endpoint Security salva eventos importantes em um arquivo de log, que pode ser exibido diretamente no menu principal do programa. Clique em **Ferramentas** > **Arquivos de log** e selecione **Log da firewall pessoal da ESET** no menu suspenso **Log**.

Os arquivos de log são uma ferramenta valiosa para detectar erros e revelar intrusos dentro do sistema. Os logs da firewall pessoal da ESET contêm os seguintes dados:

- Data e hora do evento
- Nome do evento
- Origem
- Endereço da rede de destino
- Protocolo de comunicação de rede
- Regra aplicada, ou nome do worm, se identificado
- Aplicativo envolvido
- Usuário

Uma análise completa desses dados pode ajudar a detectar tentativas de se comprometer a segurança do sistema. Muitos outros fatores indicam riscos de segurança potenciais e permitem que você reduza seus impactos: conexões muito frequentes de locais desconhecidos, diversas tentativas para estabelecer conexões, aplicativos desconhecidos comunicando-se ou números de portas incomuns sendo utilizados.

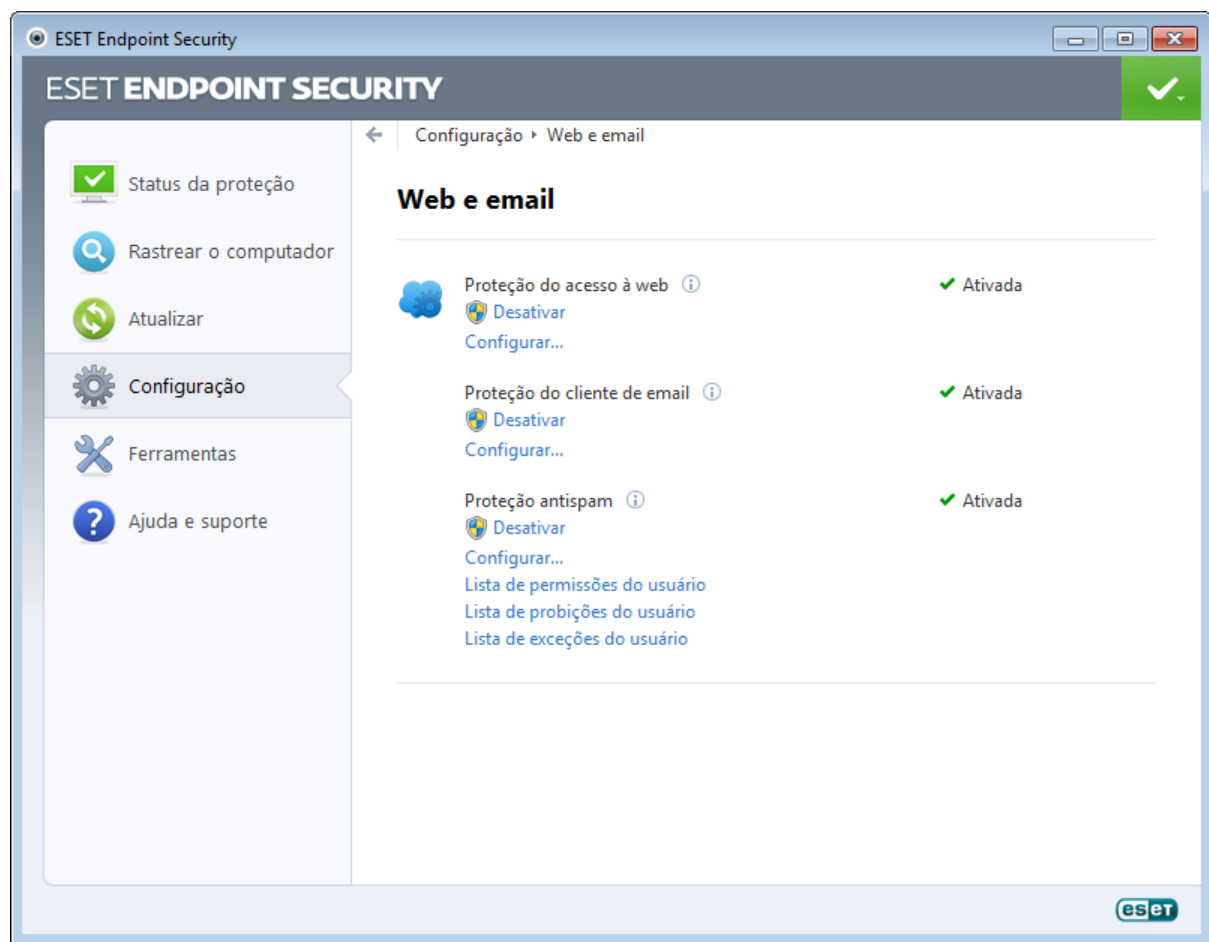
### 4.2.7 Integração do sistema

O Firewall pessoal do ESET Endpoint Security pode operar em diversos níveis:

- **Todos os recursos ativos** - O firewall pessoal está totalmente integrado e os componentes dele estão ativos (opção padrão). Caso o computador esteja conectado a uma rede maior ou à Internet, é aconselhável deixar esta opção ativada. Essa é a opção mais segura e protege totalmente seu sistema.
- **O firewall pessoal está inativo** - O firewall pessoal está integrado no sistema e faz a mediação da comunicação de rede, mas a verificação de ameaças não é executada.
- **Rastrear apenas protocolos de aplicativo** - Apenas componentes do firewall pessoal que fornecem rastreamento de protocolos de aplicativo (HTTP, POP3, IMAP e suas versões seguras) estão ativos. Se os protocolos de aplicativos não forem rastreados, a proteção será executada no nível de proteção em tempo real do sistema de arquivos e no rastreio do computador sob demanda.
- **O firewall pessoal está completamente desativado** - Selecione essa opção para remover completamente o registro do firewall pessoal no sistema. Nenhum rastreamento é executado. Isso pode ser útil ao testar - se um aplicativo for bloqueado, você poderá verificá-lo se ele for bloqueado pelo firewall. Essa é a opção menos segura, portanto recomendamos que seja cuidadoso ao desativar o firewall completamente.

**Adiar a atualização do módulo do firewall até a reinicialização do computador** - A atualização só poderá ser obtida por download. A instalação será executada durante um reinício do computador.

## 4.3 Web e email

A configuração da Web e de email pode ser encontrada no painel **Configuração** depois de clicar em **Web e email**. A partir daqui, você pode acessar mais configurações detalhadas do programa..

A conectividade com a Internet é um recurso padrão em computadores pessoais. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. Por isso, é essencial refletir com atenção sobre a **Proteção do acesso à web**.

A **Proteção do cliente de email** fornece controle da comunicação por email recebida através dos protocolos POP3 e IMAP. Usando o plug-in do cliente de email, o ESET Endpoint Security permite controlar todas as comunicações vindas através do cliente de email (POP3, MAPI, IMAP, HTTP).

A **Proteção antispam** filtra mensagens de email não solicitadas.

**Desativar** - Desativa a proteção de web/email/antispam para clientes de email.

**Configurar ...** - Abre as configurações avançadas da proteção de web/email/antispam .

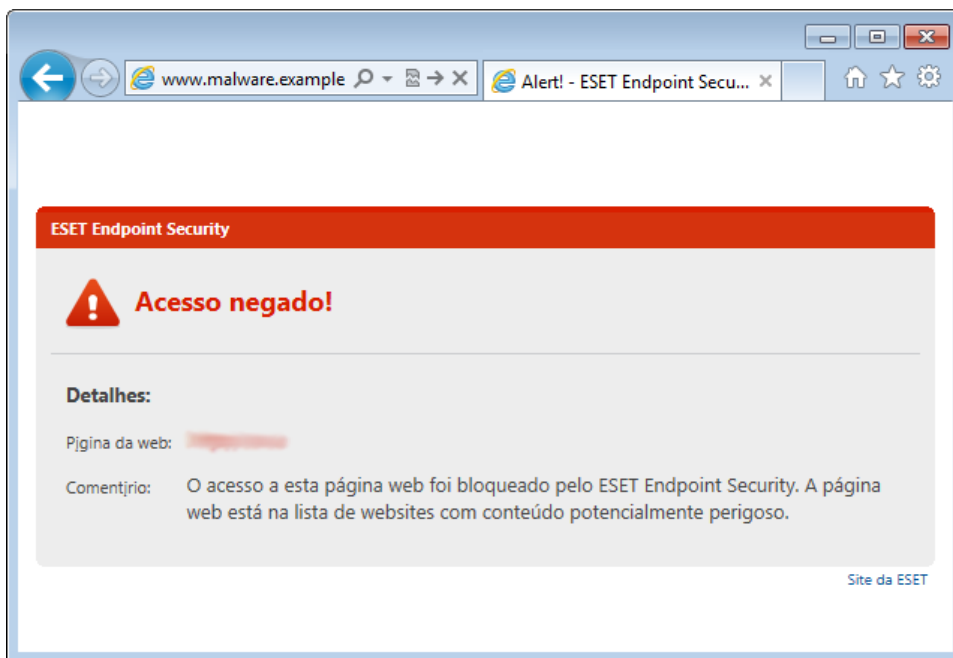
**Lista de permissões do usuário** - Abre uma janela de diálogo onde pode adicionar, editar ou excluir endereços de email considerados seguros. As mensagens de email cujos endereços de remetentes constarem na Lista de permissões não serão rastreadas quanto a spam.

**Lista de proibições** - Abre uma janela de diálogo para adicionar, editar ou excluir endereços de email considerados inseguros. As mensagens de email cujos endereços de remetentes constarem na Lista de proibições serão avaliadas como spam.

**Lista de exceções do usuário** - Abre uma janela de diálogo onde é possível adicionar, editar ou excluir endereços de email que podem ser falsos e usados para o envio de spam. As mensagens de email cujos endereços de remetentes constarem na Lista de exceções serão sempre rastreadas quanto a spam. Por padrão, a Lista de exceções contém seus endereços de email em contas existentes dos clientes de email.

### 4.3.1 Proteção do acesso à web

A conectividade com a Internet é um recurso padrão em um computador pessoal. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. Proteção do acesso à web funciona ao monitorar a comunicação entre os navegadores da web e servidores remotos e cumpre as regras do protocolo HTTP (Hypertext Transfer Protocol) e HTTPs (comunicação criptografada).

O termo roubo de identidade define uma atividade criminal que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Leia mais sobre essa atividade no glossário. O ESET Endpoint Security suporta uma proteção antiphishing reconhecendo páginas da web que com certos conteúdos serão bloquadas.

Recomendamos que Proteção do acesso à web sejam ativadas. Essa opção pode ser acessada a partir da janela principal do ESET Endpoint Security localizada em **Configuração** > **Web e email** > **Proteção do acesso à web**.

### 4.3.1.1 HTTP, HTTPs

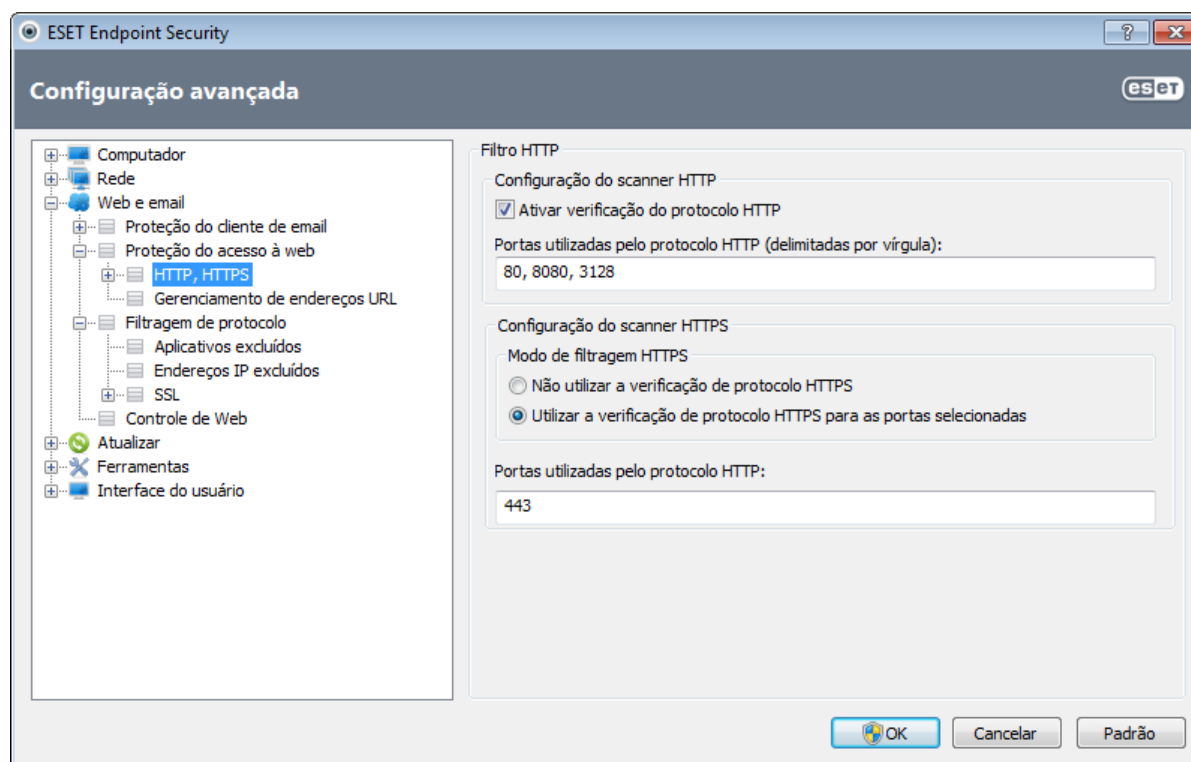
Por padrão, o ESET Endpoint Security está configurado para usar os padrões da maioria dos navegadores de Internet. Contudo, as opções de configuração do rastreamento HTTP podem ser modificadas em **Configuração avançada** (F5) > **Web e email** > **Proteção do acesso à web** > **HTTP, HTTPS**. Na janela principal **Rastreamento HTTP/HTTPS**, é possível selecionar ou desmarcar a opção **Ativar verificação de HTTP**. Você também pode definir os números das portas utilizadas para a comunicação HTTP. Por padrão, os números de portas 80 (HTTP), 8080 e 3128 (para servidor Proxy) estão predefinidos.

O ESET Endpoint Security oferece suporte à verificação do protocolo HTTPS. A comunicação HTTPS utiliza um canal criptografado para transferir as informações entre servidor e cliente. O ESET Endpoint Security verifica as comunicações utilizando os métodos de criptografia SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte). A verificação de HTTPS pode ser executada nos seguintes modos:

**Não utilizar a verificação de protocolo HTTPS** - A comunicação criptografada não será verificada.

**Utilizar a verificação de protocolo HTTPS para as portas selecionadas** - Verificação de HTTPS apenas para as portas definidas em **Portas utilizadas pelo protocolo HTTPS**.

**Utilizar a verificação de protocolo HTTPs para portas selecionadas** - O programa só verificará esses aplicativos que são especificados na seção navegadores e que utilizam as portas definidas em **Portas utilizadas pelo protocolo HTTPs**. A porta 443 é definida por padrão.

A comunicação criptografada não será rastreada. Para ativar o rastreamento da comunicação criptografada e visualizar a configuração do scanner, navegue até Verificação de protocolo SSL na seção Configuração avançada, clique em **Web e email** > **Filtragem de protocolo** > **SSL** e ative a opção **Sempre rastrear o protocolo SSL**.

#### 4.3.1.1.1 Modo ativo para navegadores da web

O ESET Endpoint Security também contém o submenu **Modo Ativo**, que define o modo de verificação para os navegadores da web.

O **Modo ativo** é útil porque ele examina os dados transferidos de aplicativos acessando a Internet como um todo, independentemente de eles serem marcados como navegadores da web ou não (para obter mais informações, consulte Clientes web e de email). Se o Modo ativo não estiver ativado, a comunicação dos aplicativos é monitorada gradualmente em lotes. Isso diminui a eficiência do processo de verificação dos dados, mas também fornece maior compatibilidade para os aplicativos listados. Se nenhum problema ocorrer ao usá-lo, recomendamos que você ative o modo de verificação ativo marcando a caixa de seleção ao lado do aplicativo desejado. O Modo ativo funciona da seguinte forma: Quando um aplicativo com acesso à rede fizer download de dados, ele será primeiro salvo em um arquivo temporário criado pelo ESET Endpoint Security. Nesse momento, os dados não estão disponíveis para o aplicativo determinado. Assim que o download for concluído, ele será rastreado contra códigos maliciosos. Se não for

encontrada infiltração, os dados serão enviados para o aplicativo original. Esse processo fornece controle completo das comunicações feitas por um aplicativo controlado. Se o modo passivo estiver ativado, os dados serão destinados ao aplicativo original para evitar atingir o tempo limite.

### 4.3.1.2 Gerenciamento de endereços URL

O gerenciamento de endereços URL permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação. Os botões **Adicionar**,**Editar**, **Remover** e **Exportar** são utilizados para gerenciar as listas de endereços. Os sites na lista de endereços bloqueados não serão acessíveis. Os sites na lista de endereços excluídos são acessados sem serem rastreados quanto a código malicioso. Se você selecionar a opção **Permitir acesso apenas a endereços URL na lista de endereços permitidos**, apenas endereços presentes na lista de endereços permitidos serão acessíveis, enquanto todos os outros endereços HTTP serão bloqueados.

Se você adicionar um endereço URL à **Lista de endereços excluídos da filtragem**, o endereço será excluído do rastreamento. Você também poderá permitir ou bloquear determinados endereços, adicionando-os à **Lista de endereços permitidos** ou **Lista de endereços bloqueados**. Depois de clicar no botão **Listas...**, a janela **Endereço HTTP/ Listas de máscaras** será exibida, na qual poderá **Adicionar** ou **Remover** listas de endereços. Para adicionar endereços URL de HTTPS à lista, a opção **Sempre rastrear o** **protocolo SSL** deverá estar ativa.

Em todas as listas, os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco substitui qualquer string de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter apenas os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista. Para ativar uma lista, selecione a opção **Lista ativa**. Se você desejar ser notificado ao inserir um endereço da lista atual, selecione **Notificar ao aplicar endereço da lista**.

ESET Endpoint Security

Configuração avançada

- Computador
- Rede
- Web e email
  - Proteção do cliente de email
  - Proteção do acesso à web
    - HTTP, HTTPS
    - Gerenciamento de endereços URL
  - Filtragem de protocolo
    - Aplicativos excluídos
    - Endereços IP excluídos
    - SSL
  - Controle de Web
- Atualizar
- Ferramentas
- Interface do usuário

Gerenciamento de endereços de URL

Ao utilizar endereço de URL/listas de máscaras, é possível especificar quais endereços serão bloqueados, permitidos ou excluídos da verificação. As listas específicas são agrupadas por tipo.

Lista de endereços excluídos da filtragem | Listas...

Permitir acesso apenas a endereços de URL na lista de endereços permitidos

Lista de endereços

Listar ativo | Notificar ao aplicar endereço da lista

*.tld*
*d?main.com*

Adicionar... | Editar... | Remover | Exportar...

OK | Cancelar | Padrão

**Adicionar.../Do arquivo** - Permite adicionar um endereço à lista manualmente (**Adicionar**) ou por meio de um arquivo de texto simples (**Do arquivo**). A opção **Do arquivo** permite adicionar diversos endereços de URL/máscaras salvos em um arquivo de texto.

**Editar...** - Edite endereços manualmente, por exemplo, adicionando uma máscara ("*" e "?").

**Remover/Remover tudo** - Clique em **Remover** para excluir os endereços selecionados da lista. Para excluir todos os endereços, selecione **Remover tudo**.

**Exportar...** - Salve endereços da lista atual em um arquivo de texto simples.

### 4.3.2 Proteção do cliente de email

A proteção de email fornece controle da comunicação por email recebida pelos protocolos POP3 e IMAP. Usando o plug-in para Microsoft Outlook e outros clientes de email, o ESET Endpoint Security permite controlar todas as comunicações vindas através do cliente de e-mail (POP3, MAPI, IMAP, HTTP). Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado oferecidos pelo mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com a base de dados de assinaturas de vírus. O rastreamento das comunicações por protocolos POP3 e IMAP é independente do cliente de email usado.

As opções dessa funcionalidade estão disponíveis em **Configuração avançada** > **Web e email** > **Proteção do cliente de email**.

**Configuração dos parâmetros do mecanismo ThreatSense** - A configuração avançada do scanner de vírus permite configurar alvos do rastreamento, métodos de detecção, etc. Clique em **Configuração...** para exibir a janela de configuração do scanner de vírus detalhada.

Depois que um email tiver sido verificado, uma notificação com o resultado da verificação pode ser anexada à mensagem. É possível selecionar **Acrescentar mensagem de marca nos emails recebidos e lidos**, bem como **Acrescentar mensagens de marca a email enviado**. Não se deve confiar nas mensagens de marca sem questioná-las, pois elas podem ser omitidas em mensagens HTML problemáticas ou podem ser forjadas por alguns vírus. As mensagens de marca podem ser adicionadas a um email recebido e lido ou a um email enviado, ou ambos. As opções disponíveis são:

- **Nunca** - nenhuma mensagem de marca será adicionada.
- **Somente para email infectado** - Somente mensagens contendo software malicioso serão marcadas como rastreadas (padrão).
- **Para todos os emails rastreados** - o programa anexará mensagens a todos os emails rastreados.

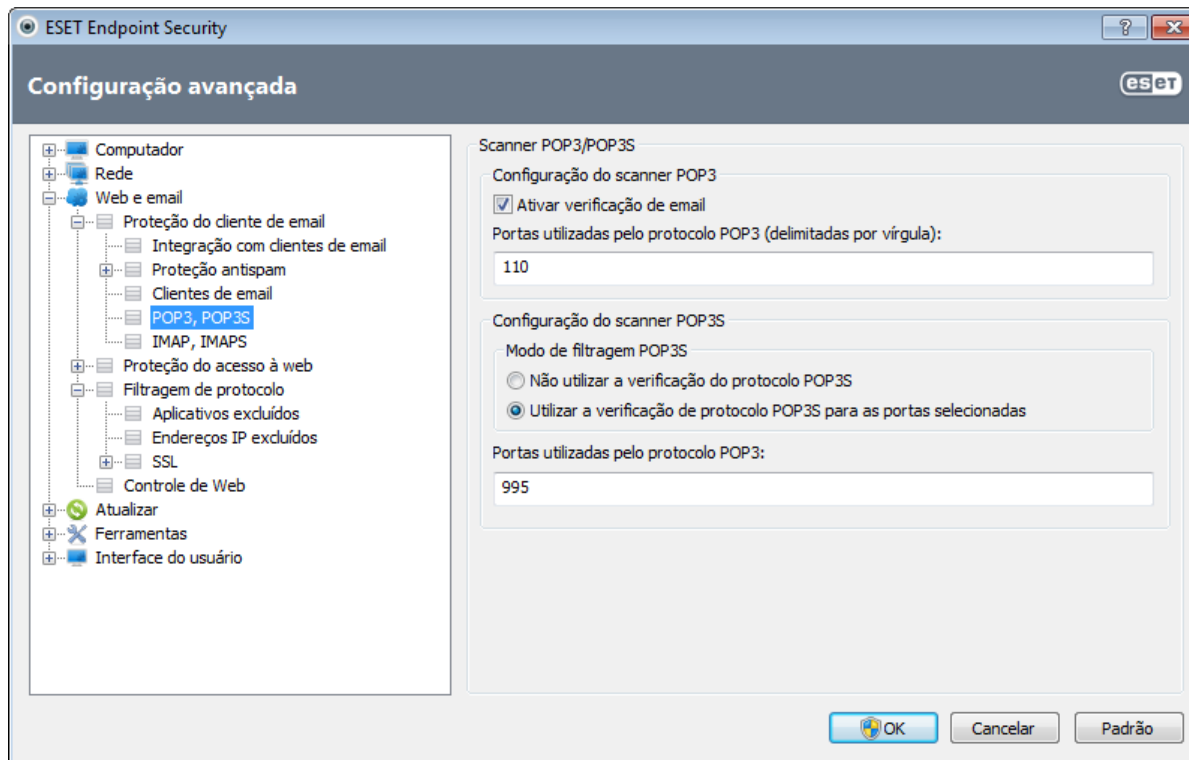
**Acrescentar observação ao assunto de email infectado recebido e lido/enviado** - Marque essa caixa de seleção se você quiser que a proteção de email inclua um alerta de vírus no assunto de um email infectado. Esse recurso permite a filtragem simples com base em assunto de email infectado (se compatível com o seu programa de email). Esse recurso aumenta o nível de credibilidade para os destinatários e, se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do email ou do remetente.

**Modelo adicionado ao assunto de email infectado** - Edite esse modelo se desejar modificar o formato de prefixo do assunto de um email infectado. Essa função substituirá o assunto da mensagem "Olá" com o prefixo "[vírus]" para o seguinte formato: "[virus] Olá". A variável %VIRUSNAME% representa a ameaça detectada.

#### 4.3.2.1 Filtro POP3, POP3S

O protocolo POP3 é o protocolo mais amplamente utilizado para receber comunicação em um aplicativo cliente de email. O ESET Endpoint Security fornece proteção a esse protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado - a verificação do protocolo POP3 é feita automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os vários números das portas devem ser delimitados por vírgula.

A comunicação criptografada não será rastreada. Para ativar o rastreamento da comunicação criptografada e visualizar a configuração do scanner, navegue até Verificação de protocolo SSL na seção Configuração avançada, clique em **Web e email** > **Filtragem de protocolo** > **SSL** e ative a opção **Sempre rastrear o protocolo SSL**.

Nesta seção, é possível configurar a verificação dos protocolos POP3 e POP3S.

**Ativar verificação do protocolo POP3** - Se estiver ativada, todo o tráfego por meio do POP3 será monitorado quanto a software malicioso.

**Portas usadas pelo protocolo POP3** - Uma lista de portas utilizadas pelo protocolo POP3 (110 por padrão).

O ESET Endpoint Security oferece também suporte à verificação do protocolo POP3S. Esse tipo de comunicação utiliza um canal criptografado para transferir as informações entre servidor e cliente. O ESET Endpoint Security verifica as comunicações utilizando os métodos de criptografia SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte).

**Não utilizar a verificação de POP3S** - A comunicação criptografada não será verificada.

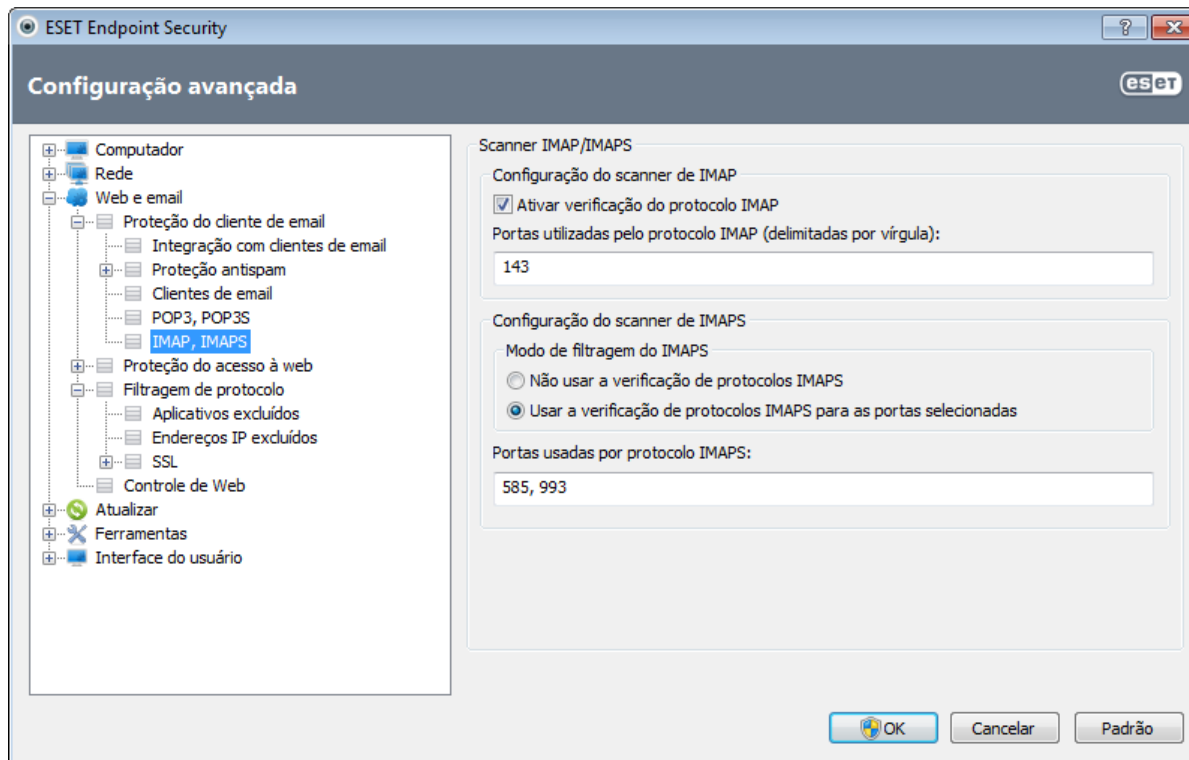
**Utilizar a verificação de protocolo POP3S para as portas selecionadas** - Selecione essa opção para permitir a verificação de POP3S apenas para as portas definidas em **Portas utilizadas pelo protocolo POP3S**.

**Portas utilizadas pelo protocolo POP3S** - Uma lista de portas POP3S a serem verificadas (por padrão, 995).

### 4.3.2.2 Protocolo de controle IMAP, IMAPS

O IMAP (Internet Message Access Protocol) é outro protocolo de Internet para recuperação de emails. O IMAP tem algumas vantagens sobre o POP3, por exemplo, vários clientes podem se conectar simultaneamente à mesma caixa de correio e gerenciar informações de estado das mensagens, tais como se a mensagem foi ou não lida, respondida ou excluída. O ESET Endpoint Security fornece proteção para este protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado; o controle do protocolo IMAP é feito automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 143 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os vários números das portas devem ser delimitados por vírgula.

A comunicação criptografada não será rastreada. Para ativar o rastreamento da comunicação criptografada e visualizar a configuração do scanner, navegue até Verificação de protocolo SSL na seção Configuração avançada, clique em **Web e email** > **Filtragem de protocolo** > **SSL** e ative a opção **Sempre rastrear o protocolo SSL**.

### 4.3.2.3 Integração com clientes de email

A integração do ESET Endpoint Security com os clientes de email aumenta o nível de proteção ativa contra códigos maliciosos nas mensagens de email. Se o seu cliente de email for compatível, essa integração poderá ser ativada no ESET Endpoint Security. Se a integração for ativada, a barra de ferramentas do ESET Endpoint Security será inserida diretamente no cliente de email, permitindo proteção mais eficiente aos emails. As configurações da integração estão disponíveis na seção **Configuração** > **Entrar na configuração avançada...** > **Web e email** > **Proteção do cliente de email** > **Integração com clientes de email**.

Os clientes de email atualmente suportados incluem o Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird. Para obter uma lista completa dos clientes de email suportados e suas versões, consulte o seguinte artigo da Base de conhecimento da ESET.

Selecione a caixa de seleção próxima a **Desativar verificação de alteração na caixa de entrada** se houver redução na velocidade do sistema ao trabalhar com o seu cliente de email. Essa situação pode ocorrer ao fazer download de email do Kerio Outlook Connector Store.

ESET Endpoint Security

Configuração avançada

Computador
Rede
Web e email
Proteção do cliente de email
Integração com clientes de email
Proteção antispam
Clientes de email
POP3, POP3S
IMAP, IMAPS
Proteção do acesso à web
Filtragem de protocolo
Aplicativos excluídos
Endereços IP excluídos
SSL
Controle de Web
Atualizar
Ferramentas
Interface do usuário

Integração com clientes de email
Integrar ao Microsoft Outlook
Integrar ao Outlook Express/Windows Mail
Integrar ao Windows Live Mail
Integrar ao Mozilla Thunderbird
Configurações especiais
Desativar verificação de alteração na caixa de entrada

OK Cancelar Padrão

Mesmo se a integração não estiver ativada, as comunicações por email ainda estarão protegidas pelo módulo de proteção do cliente de email (POP3, IMAP).

#### 4.3.2.3.1 Configuração da proteção do cliente de email

O módulo de proteção do cliente de email suporta os seguintes clientes de email: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird. A proteção de email funciona como um plug-in para esses programas. A principal vantagem do controle de plug-in é que ele não depende do protocolo usado. Quando o cliente de email recebe uma mensagem criptografada, ela é descriptografada e enviada para o scanner de vírus.

**Email para ser rastreado**

**Email recebido** - Alterna a verificação das mensagens recebidas.
**Email enviado** - Alterna a verificação das mensagens enviadas.
**Email lido** - Alterna a verificação das mensagens lidas.

**Ação que será executada no email infectado**

**Nenhuma ação** - Se ativada, o programa identificará anexos infectados, mas não será tomada qualquer ação em relação aos emails.
**Excluir email** - O programa notificará o usuário sobre infiltrações e excluirá a mensagem.
**Mover email para a pasta Itens excluídos** - Os emails infectados serão movidos automaticamente para a pasta **Itens excluídos**.
**Mover email para pasta** - Especifique a pasta personalizada para a qual você deseja mover o email infectado quando detectado.

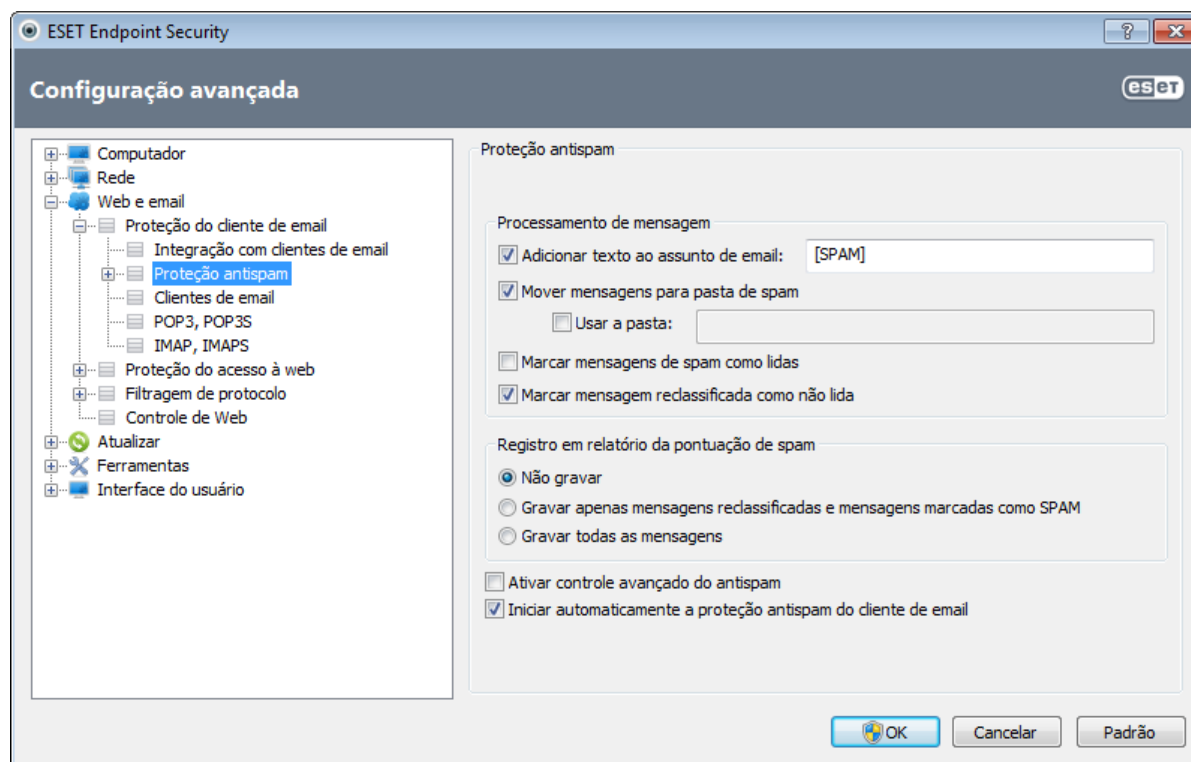
**Outros**

**Repetir o rastreamento após atualização** - Alterna o rastreamento depois de uma atualização do banco de dados de assinatura de vírus.
**Aceitar resultados de rastreamento de outros módulos** - Se essa opção for selecionada, o módulo de proteção do email aceitará os resultados de rastreamento de outros módulos de proteção.

### 4.3.2.4 Removendo infiltrações

Se receber uma mensagem de email infectada, será exibida uma janela de alerta. A janela de alerta mostra o nome do remetente, o email e o nome da infiltração. Na parte inferior da janela, as opções **Limpar**, **Excluir** ou **Deixar** estarão disponíveis para cada objeto detectado. Na maioria dos casos, recomendamos a seleção de **Limpar** ou **Excluir**. Em determinadas situações, se desejar receber o arquivo infectado, selecione **Deixar**. Se a **Limpeza rígida** estiver ativada, uma janela de informações sem nenhuma opção disponível para os objetos infectados será exibida.

### 4.3.3 Proteção antispam

Os emails não solicitados, conhecidos como spams, estão entre os maiores problemas da comunicação eletrônica. Os spams representam até 80 por cento de toda a comunicação por email. A proteção Antispam serve para proteger contra esse problema. Combinando diversos princípios eficientes, o módulo Antispam fornece filtragem superior para manter a caixa de entrada limpa.

Um princípio importante para a detecção do spam é a capacidade de reconhecer emails não solicitados com base em endereços confiáveis predefinidos (lista de permissões) e em endereços de spam (lista de proibições). Todos os endereços de sua lista de contatos são automaticamente acrescentados à lista de permissões, bem como todos os demais endereços marcados pelo usuário como seguros.

O principal método usado para detectar spam é o rastreamento das propriedades da mensagem de email. As mensagens recebidas são verificadas quanto aos critérios Antispam básicos (definições da mensagem, heurísticas estatísticas, reconhecimento de algoritmos e outros métodos únicos) e o valor do índice resultante determina se uma mensagem é spam ou não.

A proteção antispam no ESET Endpoint Security permite definir diferentes parâmetros para trabalhar com as listas de emails. As opções são:

**Iniciar automaticamente a proteção antispam do cliente de email** - Ativa/desativa a proteção antispam do cliente de email.

**Processamento de mensagens**

**Adicionar texto ao assunto de email** - Permite adicionar uma cadeia de caracteres de prefixo personalizado à linha de assunto das mensagens classificadas como spam. O padrão é "[SPAM]".

**Mover mensagens para pasta Spam** - Quando ativada, as mensagens de spam serão movidas para a pasta padrão de lixo eletrônico.

**Usar a pasta** - Esta opção move o spam para uma pasta definida pelo usuário.

**Marcar mensagens de spam como lidas** - Escolha esta opção para marcar automaticamente spam como lido. Isso o

ajudará a concentrar sua atenção em mensagens "limpas".

**Marcar mensagens reclassificadas como não lidas** - As mensagens originariamente classificadas como spam, mas posteriormente marcadas como "limpas" serão exibidas como não lidas.

**Registro em log da pontuação de spam**

O mecanismo antispam do ESET Endpoint Security atribui uma pontuação de spam a cada mensagem rastreada. A mensagem será registrada no log de antispam (**ESET Endpoint Security** > **Ferramentas** > **Arquivos de log** > **Proteção antispam**).

- **Não gravar** - A célula **Pontuação** no log da proteção antispam estará vazia.
- **Gravar apenas mensagens reclassificadas e mensagens marcadas como SPAM** - Use essa opção se desejar registrar uma pontuação de spam para mensagens marcadas como SPAM.
- **Gravar todas as mensagens** - Todas as mensagens serão registradas no log com uma pontuação de spam.

**Iniciar automaticamente a proteção antispam do cliente de email** - Quando ativada, a proteção antispam será automaticamente ativada na inicialização do sistema.

**Ativar controle avançado do antispam** - Bancos de dados antispam adicionais serão baixados, aumentando as capacidades antispam e produzindo melhores resultados.

O ESET Endpoint Security é compatível com a proteção antispam para Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.

### 4.3.3.1 Adição de endereços à lista de permissões e à lista de proibições

Emails de pessoas com quem você se comunica com frequência podem ser adicionados à lista de permissões para garantir que nenhuma mensagem desses remetentes permitidos seja classificada como spam. Endereços de spam conhecidos podem ser adicionados à lista de proibições e sempre podem ser classificados como spam. Para adicionar um novo endereço à lista de permissões ou de proibições, clique com o botão direito do mouse no email e selecione **ESET Endpoint Security** > **Adicionar à lista de permissões** ou **Adicionar à lista de proibições**, ou clique no botão **Endereço confiável** ou **Endereço de spam** na barra de ferramentas antispam do ESET Endpoint Security, em seu cliente de email.

Esse processo também se aplica aos endereços de spam. Se um endereço de email for listado na lista de proibições, cada mensagem de email enviada daquele endereço será classificada como spam.

### 4.3.3.2 Marcar mensagens como spam

Qualquer mensagem exibida em seu cliente de email pode ser marcada como spam. Para isso, clique com o botão direito do mouse na mensagem e clique em **ESET Endpoint Security** > **Reclassificar mensagens selecionadas como spam** ou clique em **Endereço de spam** na barra de ferramentas antispam do ESET Endpoint Security localizada na seção superior de seu cliente de email.

As mensagens reclassificadas são automaticamente movidas para a pasta SPAM, mas o endereço de email do remetente não é acrescentado à lista de proibições. De modo similar, as mensagens podem ser classificadas como “não spam”. Se as mensagens da pasta **Lixo eletrônico** forem classificadas como não spam, elas serão movidas para a sua pasta original. Marcar uma mensagem como não spam não acrescenta automaticamente o endereço do remetente à lista de permissões.

### 4.3.4 Filtragem de protocolos

A proteção antivírus para os protocolos dos aplicativos é fornecida pelo mecanismo de rastreamento ThreatSense, que integra perfeitamente todas as técnicas avançadas de rastreamento de malware. O controle funciona automaticamente, independentemente do navegador da Internet ou do cliente de email utilizado. Para comunicação criptografada (SSL), consulte **Filtragem de protocolo** > **SSL**.

**Ativar filtragem de conteúdo do protocolo de aplicativo** - Se ativado, todo o tráfego HTTP(S), POP3(S) e IMAP(S) será verificado pelo rastreamento antivírus.

**OBSERVAÇÃO:** Iniciando com o Windows Vista Service Pack 1 e com o Windows Server 7, a nova arquitetura WFP (Windows Filtering Platform) é utilizada para verificar a comunicação de rede. Como a tecnologia WFP utiliza técnicas especiais de monitoramento, as seguintes opções não estarão disponíveis:

- **Portas HTTP e POP3** - Limita o roteamento do tráfego ao servidor proxy interno apenas para as portas HTTP e POP3.
- **Aplicativos marcados como navegadores da web e clientes de email** - Limita o roteamento do tráfego para o servidor proxy interno somente para os aplicativos marcados como navegadores e clientes de email (**Web e email** > **Filtragem de protocolo** > **Web e clientes de email**).
- **Portas e aplicativos marcados como navegadores da Internet ou clientes de email** - Ativa o roteamento de todo o tráfego nas portas HTTP e POP3 bem como de toda a comunicação dos aplicativos marcados como navegadores da Internet e clientes de email no servidor proxy interno.

#### 4.3.4.1 Clientes web e de email

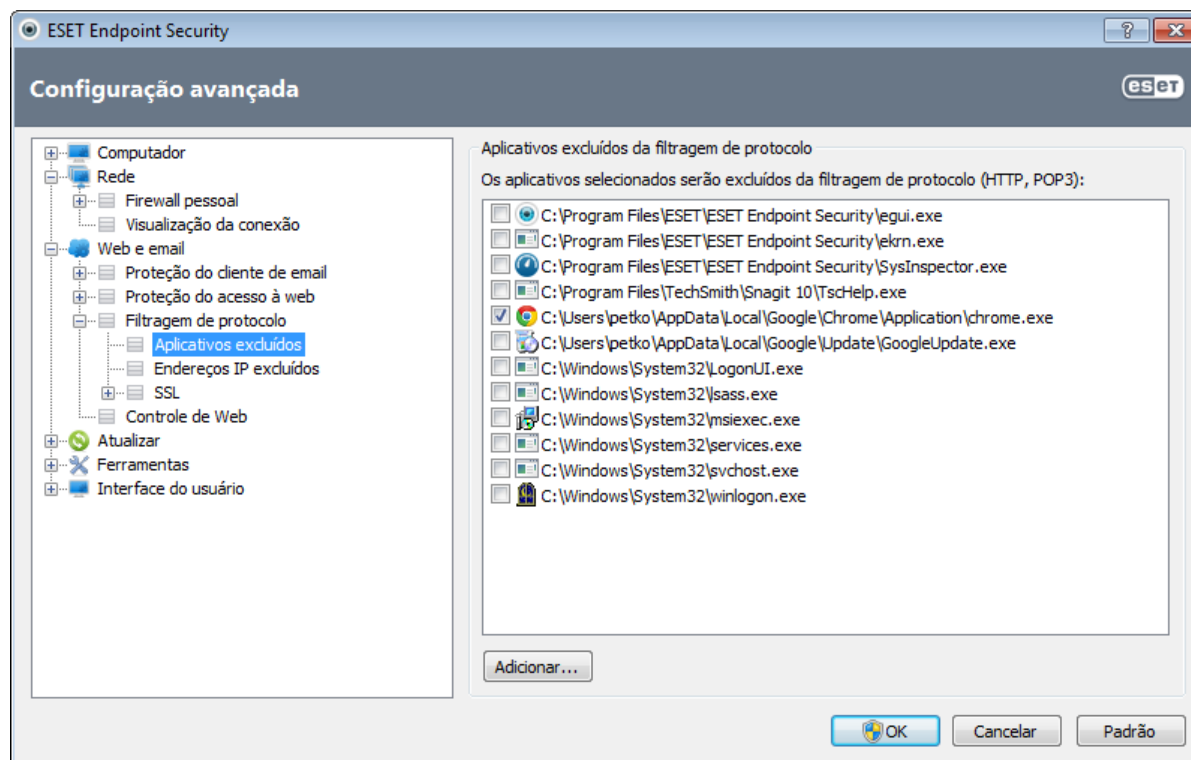
**OBSERVAÇÃO:** Iniciando com o Windows Vista Service Pack 1 e com o Windows 7, a nova arquitetura WFP (Windows Filtering Platform) é utilizada para verificar a comunicação de rede. Como a tecnologia WFP utiliza técnicas especiais de monitoramento, a seção **Clientes web e de email** não está disponível.

Devido à enorme quantidade de códigos maliciosos circulando na Internet, a navegação segura é um aspecto muito importante na proteção do computador. As vulnerabilidades do navegador da Web e os links fraudulentos ajudam o código malicioso a entrar no sistema despercebido e é por isso que o ESET Endpoint Security se focaliza na segurança do navegador da web. Cada aplicativo que acessar a rede pode ser marcado como um navegador da Internet. A caixa de seleção possui dois estados:

- **Desmarcada** - A comunicação de aplicativos é filtrada apenas para as portas especificadas.
- **Marcada** - A comunicação é sempre filtrada (mesmo que uma porta diferente seja definida).

#### 4.3.4.2 Aplicativos excluídos

Para excluir da filtragem de conteúdos a comunicação de aplicativos específicos que possuem direito de acesso à rede, selecione-os na lista. A comunicação HTTP/POP3/IMAP dos aplicativos selecionados não será verificada quanto a ameaças. Recomendamos que use essa opção somente para aplicativos que não funcionem corretamente quando a comunicação deles for verificada.

A execução de aplicativos e serviços estará disponível automaticamente. Clique no botão **Adicionar...** para selecionar manualmente um aplicativo não mostrado na lista de filtragem do protocolo.

### 4.3.4.3 Endereços IP excluídos

As entradas na lista de endereços serão excluídas da filtragem de conteúdos do protocolo. A comunicação HTTP/POP3/IMAP de/para os endereços selecionados não será verificada quanto a ameaças. Recomendamos que use essa opção apenas para endereços que sejam confiáveis.

**Adicionar endereço IPv4/IPv6** - Essa opção permite adicionar um endereço IP/intervalo de endereços/sub-rede de um ponto remoto para o qual a regra deve ser aplicada.

**Remover** - Remove as entradas selecionadas da lista.

ESET Endpoint Security
Configuração avançada
Computador
Rede
Firewall pessoal
Visualização da conexão
Web e email
Proteção do cliente de email
Proteção do acesso à web
Filtragem de protocolo
Aplicativos excluídos
Endereços IP excluídos
SSL
Controle de Web
Atualizar
Ferramentas
Interface do usuário
Endereços excluídos da filtragem de protocolo
Os endereços de IP específicos serão excluídos da filtragem de protocolo (HTTP, POP3):
Endereço: 10.1.2.3
Intervalo de endereços: 10.2.1.1 - 10.2.1.10
Sub-rede: 192.168.1.0 / 255.255.255.0
Adicionar endereço IPv4
Remover
OK
Cancelar
Padrão

#### 4.3.4.3.1 Adicionar endereço IPv4

Essa opção permite adicionar um endereço IP/intervalo de endereços/sub-rede de um ponto remoto para o qual a regra deve ser aplicada. A versão 4 do IP (Internet Protocol) é a versão mais antiga, mas ainda é a mais amplamente utilizada.

**Endereço único** - Adiciona o endereço IP de um computador individual para o qual a regra será aplicada (por exemplo, 192.168.0.10).

**Intervalo de endereços** - Digite o primeiro e último endereço IP para especificar o intervalo IP (de vários computadores) para o qual a regra será aplicada (por exemplo, 192.168.0.1 a 192.168.0.99).

**Sub-rede** - Sub-rede (um grupo de computadores) definida por um endereço IP e máscara.

Por exemplo, 255.255.255.0 é a máscara de rede para o prefixo 192.168.1.0/24, que significa o intervalo de endereços de 192.168.1.1 a 192.168.1.254.

#### 4.3.4.3.2 Adicionar endereço IPv6

Essa opção permite adicionar um endereço/sub-rede IPv6 de um ponto remoto para o qual a regra deve ser aplicada. É a versão mais recente do protocolo do IP (Internet Protocol) e substituirá a versão 4 mais antiga.

**Endereço único** - Adiciona o endereço IP de um computador individual para o qual a regra é aplicada (por exemplo 2001:718:1c01:16:214:22ff:fec9:ca5).

**Sub-rede** - A sub-rede (um grupo de computadores) é definida por um endereço IP e máscara (por exemplo: 2002:c0a8:6301:1::1/64).

#### 4.3.4.4 Verificação do protocolo SSL

O ESET Endpoint Security permite verificar protocolos encapsulados no protocolo SSL. É possível usar vários modos de rastreamento para as comunicações protegidas por SSL utilizando certificados confiáveis, certificados desconhecidos ou certificados excluídos da verificação das comunicações protegidas por SSL.

**Sempre rastrear o protocolo SSL** - Selecione essa opção para rastrear todas as comunicações protegidas por SSL, exceto as comunicações protegidas por certificados excluídos da verificação. Se uma nova comunicação que utiliza um certificado desconhecido e assinado for estabelecida, você não será notificado e a comunicação será filtrada automaticamente. Ao acessar um servidor com um certificado não confiável marcado por você como confiável (ele será adicionado à lista de certificados confiáveis), a comunicação com o servidor será permitida e o conteúdo do canal de comunicação será filtrado.

**Perguntar sobre sites não visitados (exclusões podem ser definidas)** - Se você entrar em um novo site protegido por SSL (com um certificado desconhecido), uma caixa de diálogo de seleção de ação será exibida. Esse modo permite criar uma lista de certificados SSL que serão excluídos do rastreamento.

**Não rastrear o protocolo SSL** - Se essa opção estiver selecionada, o programa não rastreará as comunicações em SSL.

**Aplicar exceções criadas com base em certificados** - Ativa o uso de exclusões especificadas em certificados excluídos e confiáveis para o rastreamento da comunicação SSL. Essa opção estará disponível se você selecionar **Sempre rastrear o protocolo SSL**.

**Bloquear comunicação criptografada utilizando o protocolo obsoleto SSL v2** - A comunicação que utiliza a versão anterior do protocolo SSL será bloqueada automaticamente.

##### 4.3.4.4.1 Certificados

Para que a comunicação SSL funcione adequadamente nos seus navegadores/clientes de email, é fundamental que o certificado raiz da ESET, spol s r.o. seja adicionado à lista de certificados raiz conhecidos (editores). Portanto, a opção **Adicionar o certificado raiz a navegadores conhecidos** deve estar ativada. Selecione essa opção para adicionar automaticamente o certificado raiz da ESET aos navegadores conhecidos (ou seja, Opera, Firefox). Para navegadores que utilizam o armazenamento de certificação do sistema, o certificado será adicionado automaticamente (ou seja, Internet Explorer). Para aplicar o certificado a navegadores não suportados, clique em **Exibir certificado** > **Detalhes** > **Copiar para arquivo...** e importe-o manualmente para o navegador.

Em alguns casos, o certificado não pode ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis (por exemplo, VeriSign). Isso significa que o certificado é assinado automaticamente por alguém (por exemplo, pelo administrador de um servidor Web ou uma empresa de pequeno porte) e considerar este certificado como confiável nem sempre é um risco. A maioria das empresas de grande porte (por exemplo, bancos) usa um certificado assinado por TRCA. Se a opção **Perguntar sobre validade do certificado** (padrão) estiver selecionada, o usuário será solicitado a selecionar uma ação a ser tomada quando for estabelecida a comunicação criptografada. Uma caixa de diálogo de seleção de ação será exibida, na qual você decidirá marcar o certificado como confiável ou excluído. Se o certificado não estiver presente na lista TRCA, a janela estará vermelha. Se o certificado estiver na lista TRCA, a janela estará verde.

Você poderá selecionar a opção **Bloquear a comunicação que utiliza o certificado** para terminar sempre uma conexão criptografada para o site que usa o certificado não verificado.

Se o certificado não for válido ou estiver corrompido, isso significa que o certificado expirou ou estava assinado incorretamente. Nesse caso, recomendamos o bloqueio da comunicação que usa o certificado.

###### 4.3.4.4.1.1 Certificados confiáveis

Além do armazenamento integrado de Autoridades de certificação raiz confiáveis, onde o ESET Endpoint Security armazena os certificados confiáveis, é possível criar uma lista personalizada de certificados confiáveis que pode ser exibida em **Configuração avançada** (F5) > **Web e email** > **Filtragem de protocolo** > **SSL** > **Certificados** > **Certificados confiáveis**. O ESET Endpoint Security verificará o conteúdo da comunicação criptografada utilizando certificados nesta lista.

Para excluir os itens selecionados da lista, clique no botão **Remover**. Clique na opção **Mostrar** (ou clique duas vezes no certificado) para exibir as informações sobre o certificado selecionado.

#### 4.3.4.4.1.2 Certificados excluídos

A seção Certificados excluídos contém certificados que são considerados seguros. O conteúdo das comunicações criptografadas que utilizam os certificados na lista não será verificado com relação a ameaças. Recomendamos excluir apenas os certificados da web que, com certeza, são seguros e a comunicação que utiliza esses certificados não precisa ser verificada. Para excluir os itens selecionados da lista, clique no botão **Remover**. Clique na opção **Mostrar** (ou clique duas vezes no certificado) para exibir as informações sobre o certificado selecionado.

#### 4.3.4.4.1.3 Comunicação SSL criptografada

Se o computador estiver configurado para rastreamento do protocolo SSL, uma janela de diálogo solicitando que você escolha uma ação pode ser aberta quando houver uma tentativa de estabelecer uma comunicação criptografada (utilizando um certificado desconhecido). A janela de diálogo contém as seguintes informações: o nome do aplicativo que iniciou a comunicação e o nome do certificado utilizado.

ESET Endpoint Security
Comunicação SSL criptografada
Certificado confiável
Um aplicativo em execução neste computador está tentando se comunicar pelo canal de SSL criptografado. Se desejar verificar o conteúdo do canal criptografado, marque o certificado como confiável.
Considera o certificado do computador remoto confiável?
Aplicativo: Google Chrome
Certificado: *.is.stuba.sk
Sim | Sim, sempre | Não
Excluir

Se o certificado não estiver localizado no armazenamento de Autoridades de certificação raiz confiáveis, ele será considerado não confiável.

ESET Endpoint Security
Comunicação SSL criptografada
Certificado não confiável
Um aplicativo em execução neste computador está tentando se comunicar pelo canal de SSL criptografado. Se desejar verificar o conteúdo do canal criptografado, marque o certificado como confiável.
Considera o certificado do computador remoto confiável?
Aplicativo: Google Chrome
Certificado: www.stuba.sk
Sim | Sim, sempre | Não
Excluir

As seguintes ações estão disponíveis para certificados:

**Sim** - O certificado será marcado temporariamente como confiável para a sessão atual - a janela de alerta não será exibida na próxima tentativa de usar o certificado.

**Sim, sempre** - Marca o certificado como confiável e adiciona-o à lista de certificados confiáveis - nenhuma janela de alerta é exibida para certificados confiáveis.

**Não** - Marca o certificado como não confiável para a sessão atual - a janela de alerta será exibida na próxima tentativa de usar o certificado.

**Excluir** - Adiciona o certificado à lista de certificados excluídos - dados transferidos por determinado canal criptografado não serão verificados.

## 4.4 Controle de Web

A seção Controle de Web permite que você defina as configurações que protegem sua empresa do risco de responsabilidade legal. Ela inclui sites que violam direitos de propriedade intelectual. O objetivo é impedir que os funcionários acessem páginas com conteúdo inadequado ou prejudicial, ou páginas que possam ter impacto negativo sobre a produtividade do trabalho.

Controle de Web permite bloquear sites que possam conter material potencialmente ofensivo. Além disso, os empregadores ou administradores do sistema podem proibir o acesso a até 27 categorias de site predefinidas e mais de 140 subcategorias.

As opções de configuração do Controle de Web podem ser modificadas em **Configuração avançada** (F5) > **Controle de Web**. A caixa de seleção ao lado de **Integrar ao sistema** integra o Controle de Web ao ESET Endpoint Security e ativa **Configurar regras...** para acessar a janela Editor de regras de controle de Web.

### 4.4.1 Regras de controle de Web

A janela **Editor de regras de controle de Web** exibe as regras existentes para endereços de URL e categorias de página da Web.

Editor de regras do Controle de Web

Defina regras para reforçar a política de uso aceitável para o uso da Internet por usuário ou por grupos de usuários. A ordem das regras define suas prioridades.

| | Ativado | Nome | Tipo | URL/Categoria | Usuários | Ação |
|---|---|---|---|---|---|---|
| 1. | ☑ | Regra sem título | Ação baseada n... | www.forbiddenpage.com | | Blo |
| 2. | ☑ | Regra sem título | Ação baseada n... | www.allowedpage.net | petko-PC\petko | Per |
| 3. | ☑ | Regra sem título | Ação baseada n... | Group 3 | | Blo |

Adicionar | Editar | Copiar | Excluir | Parte superior | Para cima | Para baixo | Parte inferior

<?xml version="1.0" encoding="utf-8"?><ESET> <RULE NAME="Regra sem tÃ-tulo" LOGSEV="0" ENABLED="1'

Editar grupo | Ok | Cancelar

A lista de regras contém diversas descrições de uma regra, tais como nome, tipo de bloqueio, ação a ser realizada após a correspondência de uma regra de controle de Web e a gravidade do relatório.

Clique em **Adicionar** ou **Editar** para gerenciar uma regra. Clique em **Copiar** para criar uma nova regra com as opções predefinidas usadas por outra regra selecionada. As cadeias XML exibidas ao clicar em uma regra podem ser copiadas para a área de transferência para ajudar os administradores do sistema a exportarem/importarem esses dados e usá-los, por exemplo no ESET Remote Administrator.

Ao pressionar CTRL e clicar, é possível selecionar mais de uma regra e aplicar as ações, tais como exclui-las ou movê-las para cima e para baixo na lista, em todas as regras selecionadas. A caixa de seleção **Ativado** desativará ou ativará uma regra; isso pode ser útil caso não deseje excluir uma regra permanentemente se você pretende usá-la no futuro.

O controle é realizado por regras classificadas na ordem que determina sua prioridade, com regras de prioridade mais alta na parte superior.

É possível clicar com o botão direito do mouse em uma regra para exibir o menu de contexto. Aqui, você pode definir o detalhamento de entradas de log (gravidade) de uma regra. As entradas de logs podem ser visualizadas a partir da janela principal do ESET Endpoint Security em **Ferramentas** > **Arquivos de log**.

Clique em **Editar grupo** para abrir a janela Editor de grupo, onde é possível adicionar e remover categorias e subcategorias predefinidas que pertençam ao grupo correspondente.

### 4.4.2 Adicionar regras de controle de Web

A janela Regras de controle de Web permite criar ou modificar manualmente uma regra de filtro do controle de Web.

Insira a descrição da regra no campo **Nome** para uma melhor identificação. A caixa de seleção **Ativado** desativa ou ativa esta regra. Isso pode ser útil caso não deseje excluir a regra permanentemente.

#### Tipo de ação

- **Ação baseada na URL** - Acesso ao site especificado. Insira o endereço URL adequado no campo **URL**.
- **Ação baseada na categoria** - Após selecionar esta opção, uma categoria do menu suspenso **Categoria** deverá ser selecionada.

Na lista de endereço URL, os símbolos especiais * (asterisco) e ? (ponto de interrogação) não podem ser usados. Por exemplo, os endereços de página da Web com vários TLDs devem ser inseridos manualmente (paginaexemplo.com, paginaexemplo.sk, etc.). Quando você insere um domínio na lista, todo o conteúdo localizado neste domínio e em todos os subdomínios (por exemplo, sub.paginaexemplo.com) será bloqueado ou permitido de acordo com sua escolha de ação baseada na URL.

#### Ação

- **Permitir** - O acesso ao endereço URL/categoria será concedido.
- **Bloquear** - Bloqueia o endereço URL/categoria.

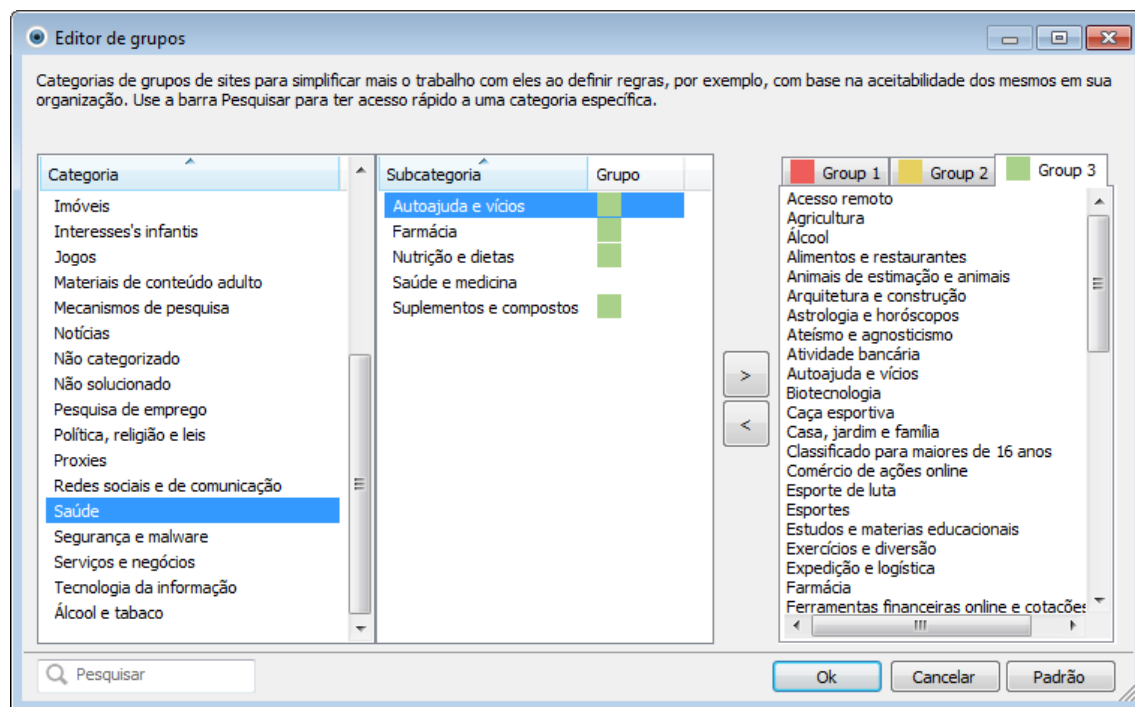
#### Lista de usuários

- **Adicionar** - Abre a janela de diálogo **Tipo de objeto: Usuários ou Grupos** que permite a seleção dos usuários desejados.
- **Excluir** - Remove o usuário selecionado do filtro.

### 4.4.3 Editor de grupo

A janela Editor de grupo é dividida em duas partes. A parte direita da janela contém uma lista de categorias e subcategorias. Selecione a categoria na lista **Categoria** para exibir suas subcategorias. A maioria das subcategorias pertence a um grupo marcado com uma cor.

O grupo de cor vermelha contém subcategorias para adultos ou geralmente inapropriadas. Por outro lado, o grupo de cor verde inclui categorias de páginas da web que podem ser consideradas aceitáveis.

Use as setas para adicionar ou remover a subcategoria selecionada para um grupo selecionado.

**Observação:** Uma subcategoria pode pertencer somente a um único grupo. Existem algumas subcategorias que não estão incluídas nos grupos predefinidos (por exemplo, Jogos). Para corresponderem a uma subcategoria desejada usando o filtro de Controle de web, adicione-a a um grupo desejado. Se a subcategoria sendo adicionada já estiver incluída em outro grupo, ela será removida e adicionada ao grupo selecionado.

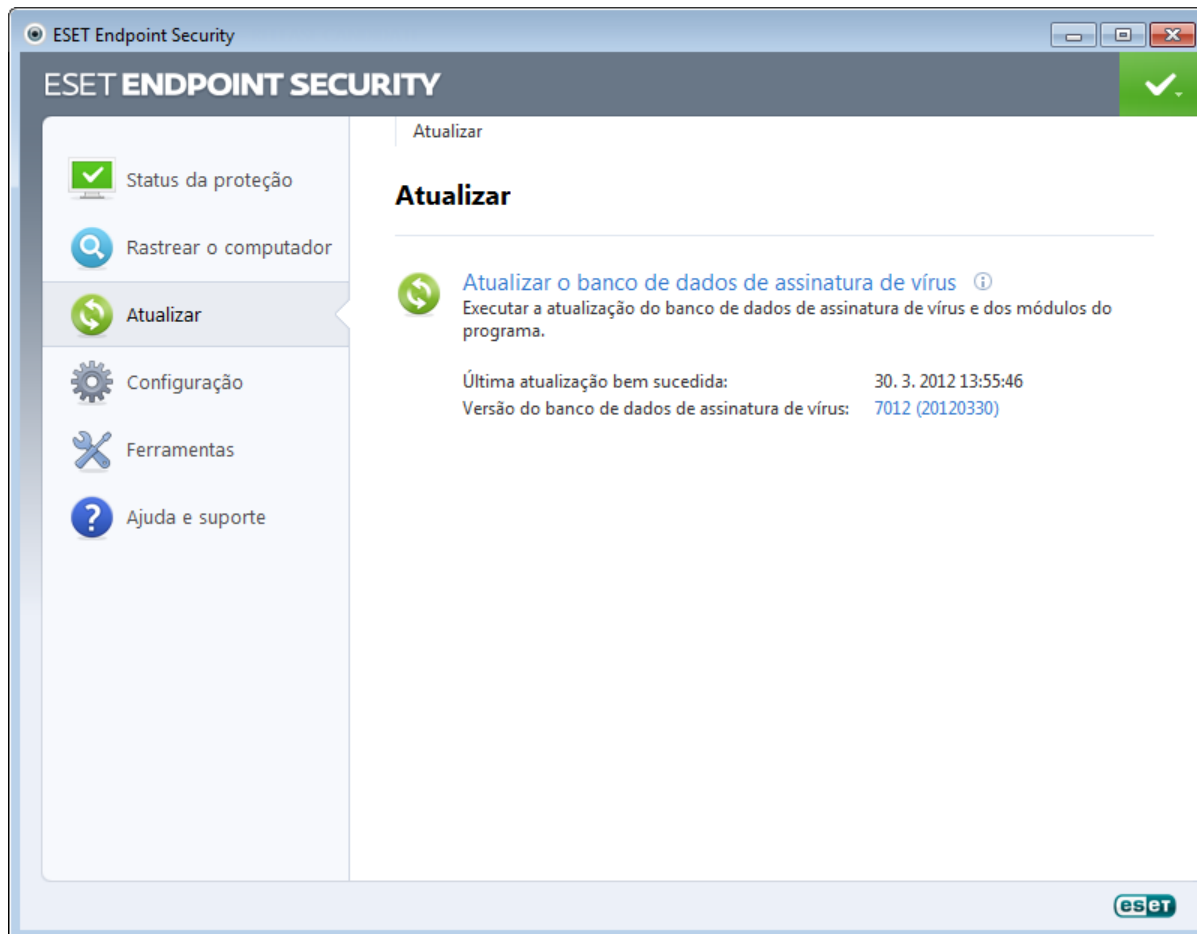
Pesquise por um grupo inserindo os termos da pesquisa no campo **Pesquisar** localizado no canto inferior esquerdo da janela.

## 4.5 Atualização do programa

Atualizar o ESET Endpoint Security periodicamente é o melhor método para se obter o nível máximo de segurança em seu computador. O módulo de atualização garante que o programa está sempre atualizado de duas maneiras, atualizando o banco de dados de assinatura de vírus e atualizando os componentes do sistema.

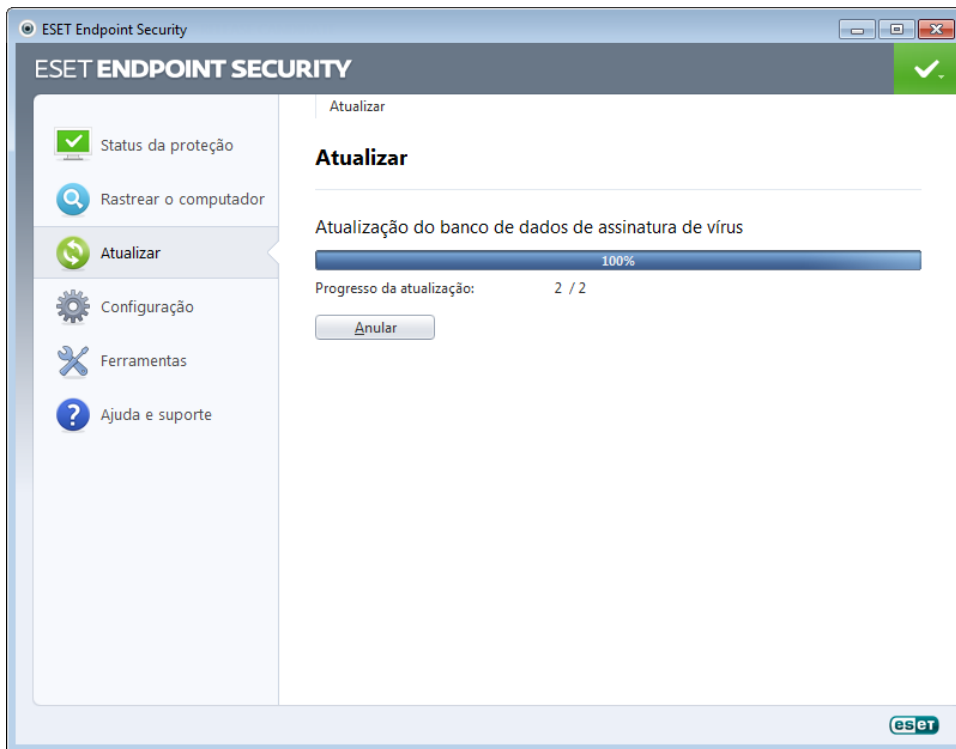
Na janela principal do programa, ao clicar em **Atualizar**, você poderá localizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida e se uma atualização será necessária. A janela principal também contém a versão do banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET que lista todas as assinaturas adicionadas em determinada atualização.

Além disso, a opção para iniciar manualmente o processo de atualização **Atualizar banco de dados de assinatura de vírus**, está disponível. A atualização do banco de dados da assinatura de vírus e a atualização dos componentes do programa são partes importantes da manutenção da proteção completa contra códigos maliciosos. Dê atenção especial à sua configuração e operação. Se você não inseriu os detalhes da licença (nome de usuário e senha) durante a instalação, você poderá inserir o nome de usuário e a senha ao atualizar para acessar os servidores de atualização da ESET.

**OBSERVAÇÃO**: Seu nome de usuário e senha são fornecidos pela ESET após a compra do ESET Endpoint Security.

**Última atualização bem-sucedida** - A data da última atualização. Verifique se ela se refere a uma data recente, o que significa que o banco de dados de assinatura de vírus está atualizado.

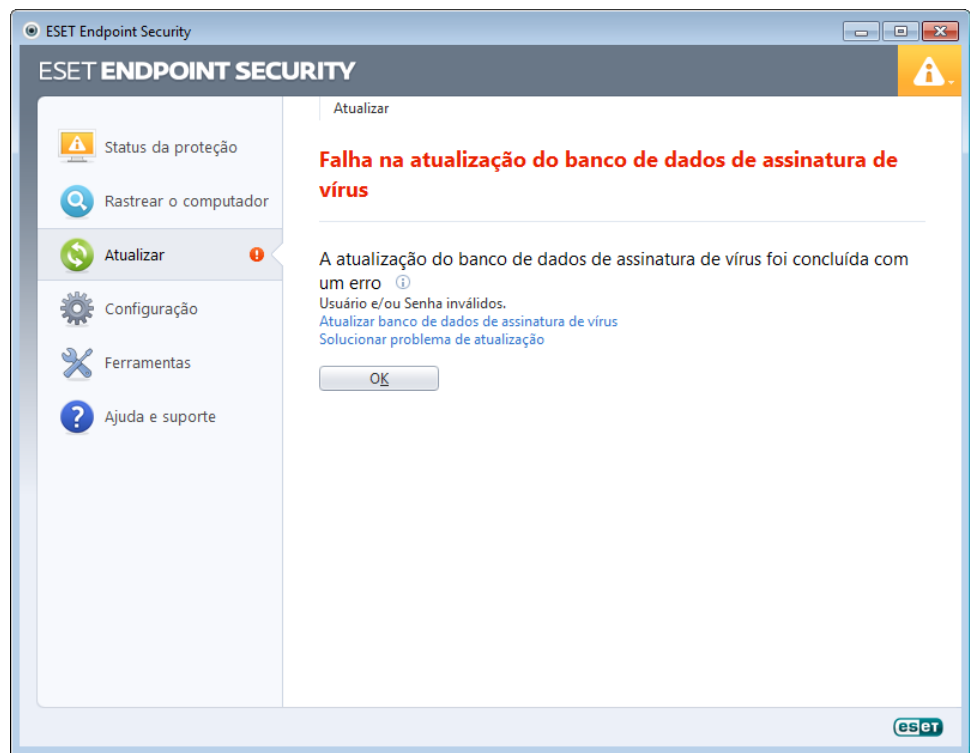
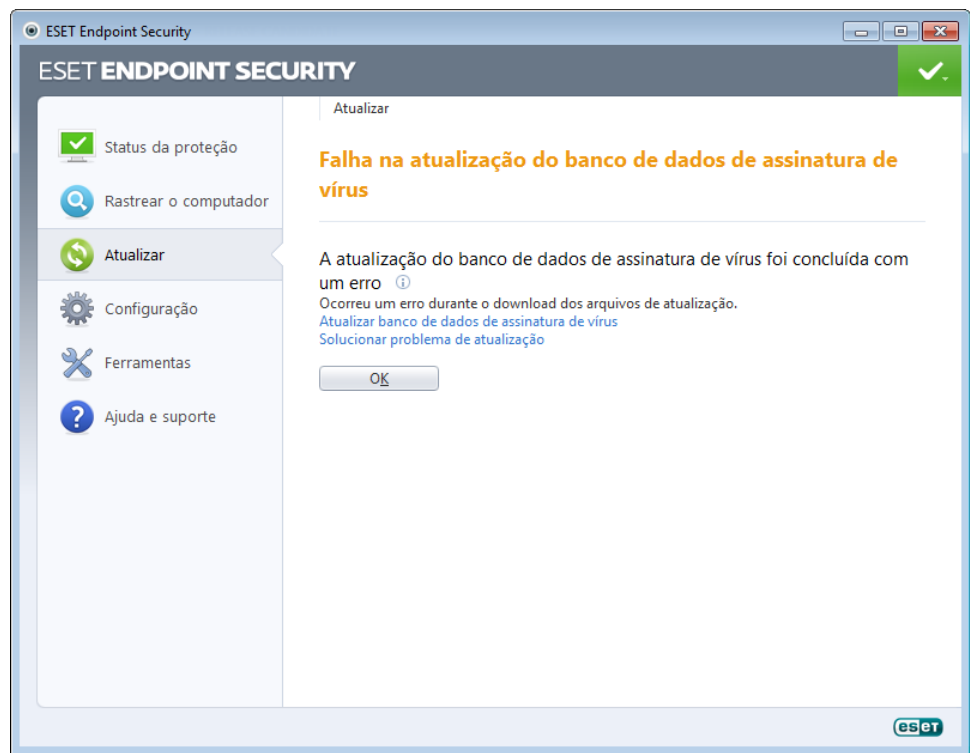
**Versão do banco de dados de assinatura de vírus** – O número do banco de dados de assinatura de vírus, que também é um link ativo para o site da ESET. Clique para exibir uma lista de todas as assinaturas adicionadas na atualização.

### Processo de atualização

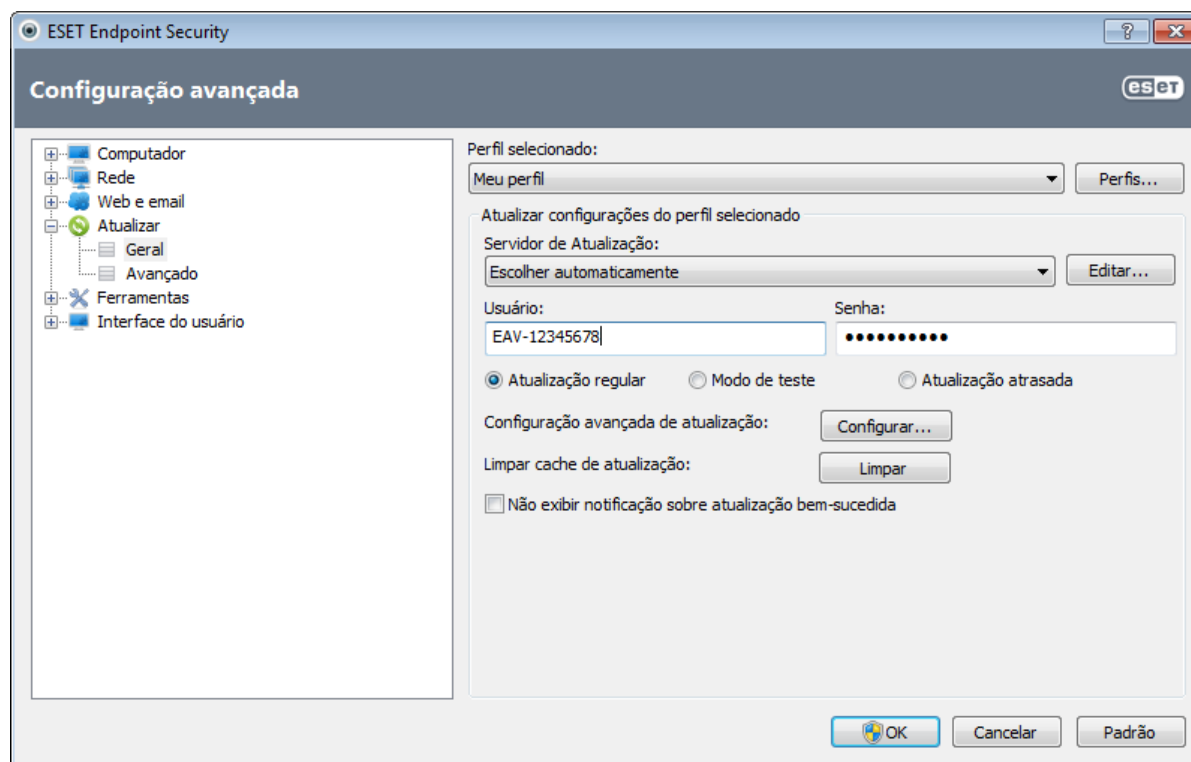
Após clicar no botão **Atualizar banco de dados de assinatura de vírus**, o processo de download é iniciado. A barra de progresso do download e o tempo restante do download serão exibidos. Para interromper a atualização, clique em **Anular**.

**Importante:** Em circunstâncias normais, quando o download das atualizações é feito adequadamente, a mensagem **A atualização não é necessária - O banco de dados de assinatura de vírus está atualizado** aparecerá na janela **Atualizar**. Se esse não for o caso, o programa estará desatualizado e mais vulnerável a uma infecção. Atualize o banco de dados de assinatura de vírus assim que for possível. Caso contrário, uma das seguintes mensagens será exibida:

**O banco de dados de assinatura de vírus está desatualizado** - Esse erro aparecerá após diversas tentativas malsucedidas de atualizar o banco de dados de assinatura de vírus. Recomendamos que você verifique as configurações de atualização. A razão mais comum para esse erro é a inserção de dados de autenticação incorretos ou as definições incorretas das configurações de conexão.

A notificação anterior está relacionada às duas mensagens a seguir de **Falha na atualização do banco de dados de assinatura de vírus** sobre atualizações malsucedidas:

1. **Usuário e/ou senha inválidos** - O nome de usuário e a senha foram inseridos incorretamente na configuração da atualização. Recomendamos que você verifique os seus dados de autenticação. A janela Configuração avançada (no menu principal, clique em **Configuração** e escolha a opção **Entrar na configuração avançada...**, ou pressione F5 no teclado) contém opções de atualização adicionais. Clique em **Atualizar** > **Geral** na árvore Configuração avançada para inserir uma nova senha e nome de usuário.

2. **Ocorreu um erro durante o download dos arquivos de atualização** - Uma possível causa do erro pode dever-se a configurações de conexão à Internet incorretas. Recomendamos que você verifique a conectividade da Internet (abrindo qualquer site em seu navegador da Web). Se o site não abrir, é provável que uma conexão com a Internet não tenha sido estabelecida ou que haja problemas de conectividade com o seu computador. Verifique com o seu provedor de serviços de Internet (ISP) se você não tiver uma conexão ativa com a Internet.

### 4.5.1 Configuração da atualização

As opções de configuração da atualização estão disponíveis na árvore **Configuração avançada** (tecla F5) clicando em **Atualizar** > **Geral**. Esta seção especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação para esses servidores. Por padrão, o menu suspenso **Servidor de atualização** está configurado para **Escolher automaticamente**, a fim de garantir que os arquivos de atualização sejam obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede.

Para que o download das atualizações seja feito de forma adequada, é fundamental preencher corretamente todos os parâmetros. Se você usar um firewall, certifique-se de que o programa tem permissão para comunicar com a Internet (p. ex., comunicação HTTP).

O perfil de atualização usado atualmente é exibido no menu suspenso **Perfil selecionado**. Clique em **Perfis...** para criar um novo perfil.

A lista de servidores de atualização disponíveis pode ser acessada por meio do menu suspenso **Servidor de atualização**. O servidor de atualização é o local onde as atualizações são armazenadas. Se você utilizar um servidor ESET, deixe a opção padrão **Escolher automaticamente** selecionada. Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações do perfil selecionado** e, em seguida, clique no botão **Adicionar**.

Ao usar um servidor HTTP local - também conhecido como Imagem - o servidor de atualização deve ser definido da seguinte forma:
http://nome_computador_ou_seu_endereço_IP:2221

Ao usar um servidor HTTP local usando SSL- o servidor de atualização deve ser definido da seguinte forma:
https://nome_computador_ou_seu_endereço_IP:2221

A autenticação dos servidores de atualização é baseada no **Usuário** e na **Senha** gerados e enviados ao usuário após a compra. Ao usar um servidor de imagem local, a verificação dependerá de sua configuração. Por padrão, não é necessário verificação, ou seja, os campos **Usuário** e **Senha** são deixados em branco.

As atualizações em modo de teste (a opção **Modo de teste**) são atualizações que passaram por testes internos e estarão disponíveis de modo geral em breve. Ao ativar as atualizações em modo de teste você pode se beneficiar do acesso aos métodos de detecção e correções mais recentes. No entanto, o modo de teste pode não ser sempre estável, e NÃO DEVE ser usado em servidores de produção e estações de trabalho em que é necessário ter a máxima disponibilidade e estabilidade. A lista dos módulos atuais pode ser encontrada em **Ajuda e suporte** > **Sobre o ESET Endpoint Security**. Se o usuário tiver apenas conhecimentos básicos, é recomendando deixar a opção padrão **Atualização regular** selecionada. Os usuários comerciais podem selecionar a opção **Atualização atrasada** para atualizar a partir de servidores especiais de atualização que fornecem novas versões do banco de dados de vírus com um atraso de, pelo menos, X horas, isto é, bancos de dados testados em um ambiente real e, por isso, considerados como estáveis.

Clique no botão **Configuração...** ao lado de **Configuração avançada de atualização** para exibir uma janela contendo as opções avançadas de atualização.

Se tiver problemas com uma atualização, clique no botão **Limpar...** para liberar a pasta com arquivos de atualização temporários.

**Não exibir notificação sobre atualização bem-sucedida** - Desativa a notificação da bandeja do sistema no canto inferior direito da tela. A seleção dessa opção será útil se um aplicativo ou jogo de tela inteira estiver em execução. Lembre-se de que o Modo de apresentação desativará todas as notificações.

#### 4.5.1.1 Atualizar perfis

Os perfis de atualização podem ser criados para várias configurações e tarefas de atualização. A criação de perfis de atualização é especialmente útil para usuários móveis, que podem criar um perfil alternativo para propriedades de conexão à Internet que mudam regularmente.

O menu suspenso **Perfil selecionado** exibe o perfil selecionado no momento, definido em **Meu perfil**, por padrão. Para criar um novo perfil, clique no botão **Perfis...** e, em seguida, clique no botão **Adicionar...** e insira seu próprio **Nome de perfil**. Ao criar um novo perfil, é possível copiar configurações de um perfil existente selecionando-o no menu suspenso **Copiar configurações do perfil**.

Na janela de configuração de perfis, é possível especificar o servidor de atualização em uma lista de servidores disponíveis ou adicionar um novo servidor. A lista de servidores de atualização existentes está localizada no menu suspenso **Servidor de atualização**. Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações do perfil selecionado** e, em seguida, clique no botão **Adicionar**.

#### 4.5.1.2 Configuração avançada de atualização

Para visualizar a Configuração avançada de atualização, clique no botão **Configuração...**. As opções de configuração avançada de atualização incluem a configuração do **Modo de atualização**, **Proxy HTTP**, **Rede** e **Imagem**.

##### 4.5.1.2.1 Modo de atualização

A guia **Modo de atualização** contém opções relacionadas à atualização do componente do programa. O programa permite que você pré-defina seu comportamento quando uma nova atualização de componentes está disponível.

As atualizações de componentes do programa oferecem novos recursos ou fazem alterações nos recursos já existentes de versões anteriores. Ela pode ser realizada automaticamente sem intervenção do usuário ou você pode escolher ser notificado. Depois de a atualização de componentes do programa ser instalada, pode ser necessário reiniciar seu computador. Na seção **Atualização de componente de programa**, três opções estão disponíveis:

- **Nunca atualizar componentes do programa** - As atualizações de componentes do programa não serão realizadas. Esta opção é adequada para instalações de servidor, pois os servidores podem geralmente ser reiniciados somente quando estiverem em manutenção.
- **Sempre atualizar componentes do programa** - As atualizações de componentes do programa serão obtidas por download e instaladas automaticamente. Lembre-se de que pode ser necessário reiniciar o computador.
- **Perguntar antes de fazer download dos componentes do programa** - Opção padrão. Você será solicitado a confirmar ou recusar as atualizações de componentes do programa quando elas estiverem disponíveis.

Após a atualização de componentes do programa, poderá ser necessário reinicializar o computador para obter uma completa funcionalidade de todos os módulos. A seção **Reiniciar depois da atualização do componente do programa** permite que o usuário selecione uma das três opções a seguir:

- **Nunca reiniciar o computador** - Não será solicitada a reinicialização, mesmo quando for necessária. Observe que isso não é recomendável, pois o computador pode não funcionar adequadamente até a próxima reinicialização.
- **Sugerir opção de reinicialização do computador, se necessário** - Opção padrão. Depois de uma atualização dos componentes do programa, uma janela de diálogo solicitará que você reinicie o computador.
- **Se necessário, reiniciar o computador sem notificar** - Depois de uma atualização dos componentes do programa, o seu computador será reiniciado (se necessário).

**OBSERVAÇÃO:** A seleção da opção mais apropriada depende da estação de trabalho em que as configurações serão aplicadas. Esteja ciente de que há diferenças entre estações de trabalho e servidores; por exemplo, reiniciar o servidor automaticamente após uma atualização de programa pode provocar danos sérios.

Se a opção **Perguntar antes de fazer download da atualização** estiver marcada, uma notificação será exibida quando uma nova atualização estiver disponível.

Se o tamanho do arquivo de atualização for maior que o valor especificado no campo **Perguntar se um arquivo de atualização for maior que**, o programa exibirá uma notificação.

#### 4.5.1.2.2 Servidor proxy

Para acessar as opções de configuração do servidor proxy de determinado perfil de atualização, clique em **Atualizar** na árvore Configuração avançada (F5) e clique no botão **Configuração...** à direita de **Configuração avançada de atualização**. Clique na guia **Proxy HTTP** e selecione uma das três opções a seguir:

- **Usar configurações globais de servidor proxy**
- **Não usar servidor proxy**
- **Conexão através de um servidor proxy**

Selecione a opção **Usar configurações globais de servidor proxy** para usar as opções de configuração do servidor proxy já especificadas na ramificação **Ferramentas** > **Servidor proxy** da árvore Configuração avançada.

Selecione a opção **Não usar servidor proxy** para especificar que nenhum servidor proxy será usado para atualizar o ESET Endpoint Security.

A opção **Conexão através de um servidor proxy** deve ser selecionada se:

- Deve ser usado um servidor proxy para atualizar o ESET Endpoint Security que seja diferente do servidor proxy especificado nas configurações globais (**Ferramentas** > **Servidor proxy**). Nesse caso, as configurações devem ser especificadas aqui: O endereço do **Servidor proxy**, a **Porta** de comunicação, além do **Usuário** e **Senha** para o servidor proxy, se necessário.
- As configurações do servidor proxy não foram definidas globalmente, mas o ESET Endpoint Security irá estabelecer conexão com um servidor proxy para atualizações.
- Seu computador estabelece conexão com a Internet por meio de um servidor proxy. As configurações são obtidas do Internet Explorer durante a instalação do programa; no entanto, se forem alteradas posteriormente (por exemplo, se você alterar o seu provedor de Internet), verifique se as configurações do proxy HTTP estão corretas nesta janela. Caso contrário, o programa não conseguirá estabelecer uma conexão com os servidores de atualização.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

**OBSERVAÇÃO:** Os dados de autenticação, tais como **Usuário** e **Senha**, são destinados para acessar o servidor proxy. Preencha esses campos somente se um nome de usuário e uma senha forem necessários. Observe que esses campos não são para seu nome de usuário/senha do ESET Endpoint Security e devem ser fornecidos somente se você souber que precisa de senha para acessar a Internet por meio de um servidor proxy.

#### 4.5.1.2.3 Conexão à rede

Ao atualizar a partir de um servidor local com um sistema operacional baseado em NT, a autenticação para cada conexão de rede é necessária por padrão. Na maioria dos casos, a conta do sistema local não tem direitos de acesso suficientes para a pasta Imagem, que contém cópias dos arquivos de atualização. Se esse for o caso, insira o nome de usuário e a senha na seção de configuração da atualização ou especifique uma conta na qual o programa acessará o servidor de atualização (Imagem).

Para configurar essa conta, clique na guia **Rede**. A seção **Conectar na rede como** fornece as opções **Conta do sistema (padrão)**, **Usuário atual** e **Usuário especificado**.

Selecione a opção **Conta do sistema (padrão)** para utilizar a conta do sistema para autenticação. De maneira geral, nenhum processo de autenticação ocorre normalmente se não houver dados de autenticação na seção principal de configuração de atualização.

Para assegurar que o programa é autenticado usando uma conta de usuário conectado no momento, selecione **Usuário atual**. A desvantagem dessa solução é que o programa não é capaz de conectar-se ao servidor de atualização se nenhum usuário tiver feito logon no momento.

Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação. Use esse método quando a conexão com a conta do sistema padrão falhar. Lembre-se de que a conta do usuário especificado deve ter acesso ao diretório de arquivos de atualização no servidor local. Caso contrário, o programa não poderá estabelecer conexão e fazer download das atualizações.

**Aviso**: Quando a opção **Usuário atual** ou **Usuário especificado** estiver selecionada, um erro poderá ocorrer ao alterar a identidade do programa para o usuário desejado. Recomendamos inserir os dados de autenticação da rede na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: nome_domínio\usuário (se for um grupo de trabalho, insira o nome_do_grupo_de_trabalho\nome) e a senha. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação

é necessária.

Selecione a opção **Desconectar do servidor depois da atualização** se a conexão com o servidor permanecer ativa mesmo depois de fazer o download das atualizações.

#### 4.5.1.2.4 Criação de cópias de atualização - Imagem

O ESET Endpoint Security permite criar cópias dos arquivos de atualização, que podem ser usadas para atualizar outras estações de trabalho localizadas na rede. Criação de uma "imagem" - uma cópia dos arquivos de atualização no ambiente de rede local é conveniente, pois os arquivos de atualização não precisam ser obtidos por download a partir do servidor de atualização da ESET repetidamente e por cada estação de trabalho. O download é feito de forma centralizada para o servidor de imagem local e, em seguida, distribuído a todas as estações de trabalho, evitando assim o risco de sobrecarga potencial do tráfego de rede. A atualização das estações clientes a partir de uma Imagem otimiza o equilíbrio de carga da rede e economiza a largura de banda da conexão com a Internet.

As opções de configuração do servidor local da Imagem podem ser acessadas (após a inserção da chave de licença válida no gerenciador de licenças, localizado na seção Configuração avançada do ESET Endpoint Security) na secção Configuração avançada de atualização. Para acessar essa seção, pressione F5 e clique em **Atualizar** na árvore Configuração avançada, depois clique no botão **Configuração...** ao lado de **Configuração avançada de atualização** e selecione a guia **Imagem**.

Configuração avançada

Modo de atualização | Proxy HTTP | Rede | Imagem

Criar imagem da atualização

Acesso para atualizar arquivos

Fornecer arquivos de atualização através do servidor HTTP

Configuração avançada...

Pasta para armazenar arquivos da imagem:

C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror

Pasta...

Usuário:

Senha:

Arquivos

Versões disponíveis:

ESET NOD32 Antivirus (Portuguese Brasil, 32bit)

ESET Smart Security (Portuguese Brasil, 32bit)

ESET NOD32 Antivirus (Portuguese Brasil, 64bit)

ESET Smart Security (Portuguese Brasil, 64bit)

OK | Cancelar

A primeira etapa na configuração da Imagem é selecionar a opção **Criar imagem de atualização**. A seleção dessa opção ativa as outras opções de configuração da Imagem, como o modo em que os arquivos de atualização serão acessados e o caminho de atualização para os arquivos da imagem.

**Fornecer arquivos de atualização através do servidor HTTP interno** - Se esta opção for ativada, os arquivos de atualização podem simplesmente ser acessados por meio de HTTP e nenhum nome de usuário e senha serão necessários aqui. Clique em Configuração avançada... para configurar as opções adicionais de imagem.

**Observação:** O servidor HTTP requer SP2 e versões posteriores no Windows XP.

Os métodos de ativação da Imagem estão descritos em detalhes na seção Atualização através da Imagem. Por enquanto, observe que há dois métodos básicos para acessar a Imagem - a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou através de um servidor HTTP.

A pasta dedicada a armazenar os arquivos de atualização para a Imagem é definida na seção **Pasta para armazenar arquivos da imagem**. Clique em **Pasta...** para procurar uma pasta no computador local ou em uma pasta de rede compartilhada. Se a autorização para a pasta especificada for necessária, os dados de autenticação devem ser inseridos nos campos **Usuário** e **Senha**. Se a pasta de destino selecionada estiver localizada em um disco de rede que esteja executando o sistema operacional Windows NT/2000/XP, o nome de usuário e a senha especificados devem ter privilégios de gravação para a pasta selecionada. O nome de usuário e a senha devem ser inseridos no formato Domínio/Usuário ou Grupo de trabalho/Usuário. Lembre-se de fornecer as senhas correspondentes.

Ao configurar a Imagem, também é possível especificar as versões de idioma dos quais se deseja fazer download das

cópias de atualização que, atualmente, são suportadas pelo servidor de imagem configurado pelo usuário. A configuração da versão de idioma pode ser acessada na lista **Versões disponíveis**.

#### 4.5.1.2.4.1 Atualização através da Imagem

Há dois métodos básicos para configurar a Imagem, a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou como um servidor HTTP.

**Acesso à Imagem utilizando um servidor HTTP interno**

Essa é a configuração padrão especificada na configuração do programa predefinida. Para permitir o acesso à imagem utilizando o servidor HTTP, navegue até **Configuração avançada de atualização** (clique na guia **Imagem**) e selecione a opção **Criar imagem da atualização**.

Na seção **Configuração avançada** da guia **Imagem**, é possível especificar a **Porta do servidor**, em que o servidor HTTP escutará, bem como o tipo de **Autenticação** usada pelo servidor HTTP. Por padrão, a porta do servidor está definida em **2221**. A opção **Autenticação** define o método de autenticação usado para acessar os arquivos de atualização. As opções disponíveis são: **NENHUM**, **Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação através de nome de usuário e senha. A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado. A configuração padrão é **NENHUM**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.

**Aviso:** Se deseja permitir acesso aos arquivos de atualização através do servidor HTTP, a pasta Imagem deve estar localizada no mesmo computador que a instância do ESET Endpoint Security que os criou.

Acrescente o **Arquivo de encadeamento do certificado** ou gere um certificado assinado automaticamente caso deseje executar o servidor HTTP com suporte HTTPS (SSL). Os seguintes tipos estão disponíveis: **ASN**, **PEM** e **PFX**. É possível fazer download dos arquivos de atualização através do protocolo HTTPS, que fornece mais segurança. É quase impossível rastrear transferências de dados e credenciais de login usando esse protocolo. A opção **Tipo chave privada** é definida como **Integrada** por padrão (e, portanto, a opção **Arquivo da chave privada** é desativada por padrão), o que significa que a chave privada é uma parte do arquivo de encadeamento do certificado selecionado.

Após concluir a configuração da Imagem, vá até as estações de trabalho e adicione um novo servidor de atualização. Para fazer isso, siga as etapas a seguir:

- Abra a **Configuração avançada do ESET Endpoint Security** e clique em **Atualizar** > **Geral**.
- Clique em **Editar...** à direita do menu suspenso **Servidor de atualização** e adicione um novo servidor usando um dos seguites formatos:
  http://endereço_IP_do_seu_servidor:2221
  https://Endereço_IP_do_servidor:2221 (se SSL for usado)
- Selecione o servidor recém-adicionado na lista de servidores de atualização.

**Acesso à Imagem por meio de compartilhamentos de sistema**

Primeiro, uma pasta compartilhada deve ser criada em um dispositivo de rede ou local. Ao criar a pasta para a Imagem, é necessário fornecer acesso de "gravação" para o usuário que salvará os arquivos de atualização na pasta e acesso de "leitura" para todos os usuários que atualizarão o ESET Endpoint Security a partir da pasta Imagem.

Em seguida, configure o acesso à Imagem na seção **Configuração avançada de atualização** da guia **Imagem** desativando a opção **Fornecer arquivos de atualização através do servidor HTTP interno**. Essa opção está ativada por padrão no pacote de instalação do programa.

Se a pasta compartilhada estiver localizada em outro computador na rede, será necessário inserir os dados de autenticação para acessar o outro computador. Para inserir os dados de autenticação, abra o ESET Endpoint Security **Configuração avançada** (F5) e clique em **Atualizar** > **Geral**. Clique no botão **Configuração...** e clique na guia **Rede**. Essa configuração é a mesma para a atualização, conforme descrito na seção Conexão à rede.

Após concluir a configuração da Imagem, prossiga até as estações de trabalho e configure \\UNC\PATH como o servidor de atualização. Essa operação pode ser concluída seguindo estas etapas:

- Abra a Configuração avançada do ESET Endpoint Security e clique em **Atualizar** > **Geral**.
- Clique em **Editar...** ao lado de servidor de atualização e adicione o novo servidor usando o formato \\UNC\CAMINHO .
- Selecione esse servidor recém-adicionado na lista de servidores de atualização.

**OBSERVAÇÃO**: Para o funcionamento correto, o caminho para a pasta Imagem deve ser especificado como um caminho UNC. A atualização das unidades mapeadas pode não funcionar.

A última seção controla os componentes do programa (PCUs). Por padrão, os componentes de programas baixados são preparados para copiar para a imagem local. Se a caixa de seleção ao lado de **Atualizar componentes do programa** estiver selecionada, não é necessário clicar em **Atualizar componentes** porque os arquivos são copiados para a imagem local automaticamente quando estiverem disponíveis. Consulte Modo de atualização para obter mais informações sobre as atualizações dos componentes do programa.

### 4.5.1.2.4.2 Solução de problemas de atualização através da Imagem

Na maioria dos casos, os problemas que ocorrem durante a atualização do servidor de imagem são causados por um ou mais dos seguintes itens: especificação incorreta das opções da pasta Imagem, dados de autenticação incorretos para a pasta Imagem, configuração incorreta nas estações de trabalho locais que tentam fazer download de arquivos de atualização a partir da Imagem ou por uma combinação das razões citadas. A seguir, é fornecida uma visão geral dos problemas mais frequentes que podem ocorrer durante uma atualização da Imagem:

O **ESET Endpoint Security relata um erro ao conectar a um servidor de imagem** - provavelmente provocado pela especificação incorreta do servidor de atualização (caminho de rede para a pasta Imagem), a partir do qual as estações de trabalho locais fazem download de atualizações. Para verificar a pasta, clique no menu **Iniciar** do Windows, clique em **Executar**, insira o nome da pasta e clique em **OK**. O conteúdo da pasta deve ser exibido.

O **ESET Endpoint Security requer um nome de usuário e senha** - Provavelmente provocado por dados de autenticação incorretos (nome de usuário e senha) na seção de atualização. O nome do usuário e a senha são utilizados para garantir acesso ao servidor de atualização, a partir do qual o programa se atualizará. Verifique se os dados de autenticação estão corretos e inseridos no formato correto. Por exemplo, Domínio/Nome de usuário ou Grupo de trabalho/Nome de usuário, além das senhas correspondentes. Se o servidor de imagem puder ser acessado por “Todos”, esteja ciente de que isso não significa que o acesso é garantido a qualquer usuário. “Todos” não significa qualquer usuário não autorizado, apenas significa que a pasta pode ser acessada por todos os usuários do domínio. Como resultado, se a pasta puder ser acessada por “Todos”, um nome de usuário e uma senha do domínio ainda precisarão ser inseridos na seção de configuração da atualização.

O **ESET Endpoint Security relata um erro ao conectar a um servidor de imagem** - A comunicação na porta definida para acessar a versão HTTP da Imagem está bloqueada.

### 4.5.1.3 Rollback de atualização

Caso suspeite que uma nova atualização do banco de dados de vírus esteja instável ou corrompida, será possível reverter para uma versão anterior e desativar quaisquer atualizações por um período de tempo desejado. Alternativamente, será possível ativar atualizações desativadas anteriormente.

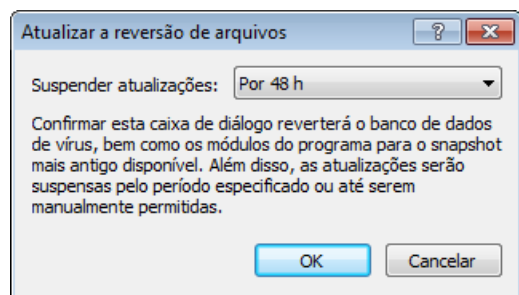
O ESET Endpoint Security fornece o backup e a restauração de módulos (chamados de reversão) do banco de dados de vírus. Para criar instantâneos do banco de dados de vírus, deixe a caixa de seleção **Criar snapshots dos arquivos de atualização** marcada. O campo **Número de instantâneos armazenados localmente** define o número de instantâneos do banco de dados de vírus anterior armazenado no sistema de arquivos do computador local.

Se você clicar em **Reverter** (**Configuração avançada** (F5) > **Atualizar** > **Avançada**), você terá que selecionar um intervalo de tempo no menu suspenso **Suspender atualizações** que represente o período de tempo que o banco de dados da assinatura de vírus e as atualizações do módulo do programa serão pausadas.

Atualizar a reversão de arquivos

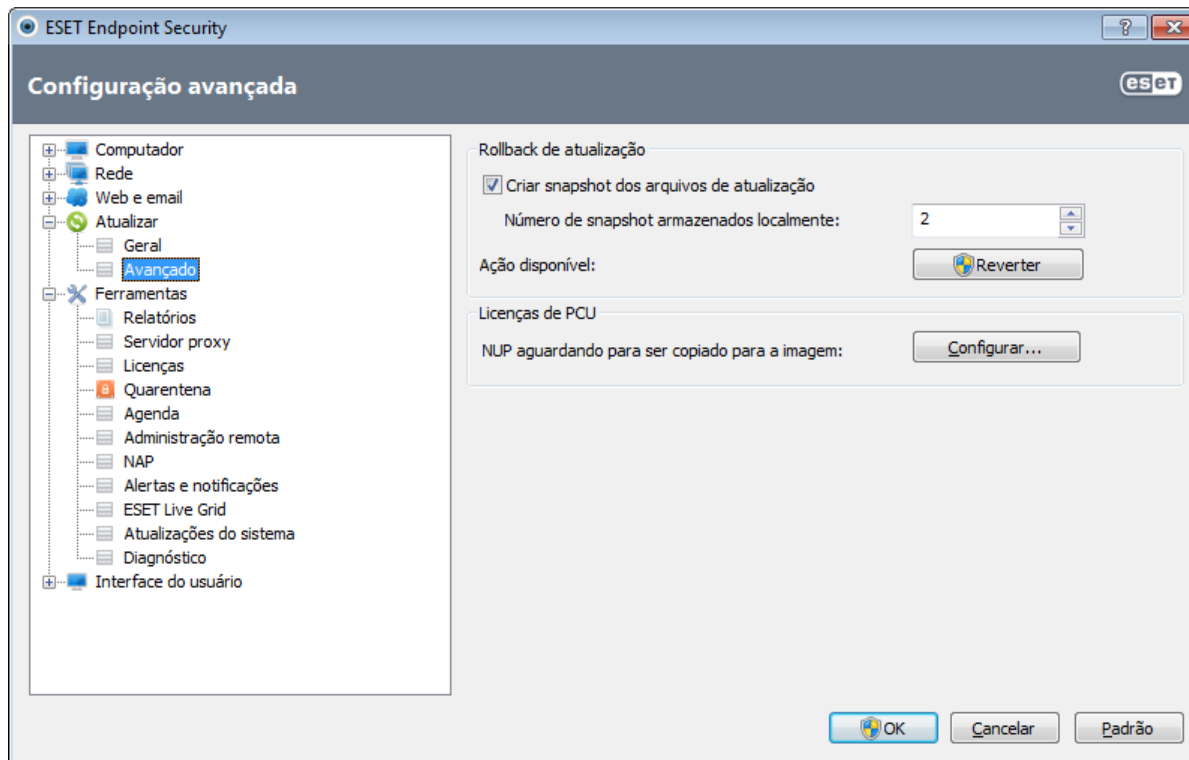
Suspender atualizações: Por 48 h

Confirmar esta caixa de diálogo reverterá o banco de dados de vírus, bem como os módulos do programa para o snapshot mais antigo disponível. Além disso, as atualizações serão suspensas pelo período especificado ou até serem manualmente permitidas.

OK Cancelar

Selecione **Até a revogação** caso deseje permitir atualizações regulares manualmente. Pois isso representa um risco de segurança em potencial, não recomendamos a seleção desta opção.

Se uma reversão estiver ativada, o botão **Reverter** se tornará **Permitir atualizações**. Nenhuma atualização será permitida durante o intervalo de tempo selecionado no menu suspenso Intevalo de tempo. A versão do banco de dados de assinatura de vírus é desatualizada para a versão mais antiga disponível e armazenada como um instantâneo no sistema de arquivos do computador local.

**Exemplo:** Permita que o número 6871 seja a versão mais atual do banco de dados de assinatura de vírus. 6870 e 6868 são armazenados como instantâneos do banco de dados de assinatura de vírus. Observe que 6869 não está disponível porque, por exemplo, o computador foi desligado por mais tempo. Se você inseriu 2 (dois) no campo **Número de instantâneos armazenados localmente** e clicou em **Reverter**, o banco de dados de assinatura de vírus será restaurado para a versão número 6868. Este processo pode demorar algum tempo. Verifique se a versão do banco de dados de assinatura de vírus foi desatualizada na janela principal do programa do ESET Endpoint Security na seção Atualizar.

As opções de configuração do servidor local da Imagem podem ser acessadas após a inserção da chave de licença válida no gerenciador de licenças, localizado na seção Configuração avançada do ESET Endpoint Security. Se você utilizar sua estação de trabalho como um mirror, as cópias de atualização deverão ter o Contrato de licença de usuário final (EULA) mais recente aceito, antes de serem criadas como arquivos de atualização de cópia para atualizar as outras estações de trabalho localizadas na rede. Se uma nova versão do EULA estiver disponível durante a atualização, uma janela de diálogo com tempo limite de 60 segundos será exibida para confirmação. Para fazer isso manualmente, clique em **Configuração...** na seção **Licenças de PCU** desta janela.

### 4.5.2 Como criar tarefas de atualização

As atualizações podem ser acionadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela principal, exibida depois de clicar em **Atualizar** no menu principal.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas estão ativadas no ESET Endpoint Security:

- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**

Toda tarefa de atualização pode ser modificada para atender às suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a seção Agenda.

## 4.6 Ferramentas

O menu **Ferramentas** inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados.

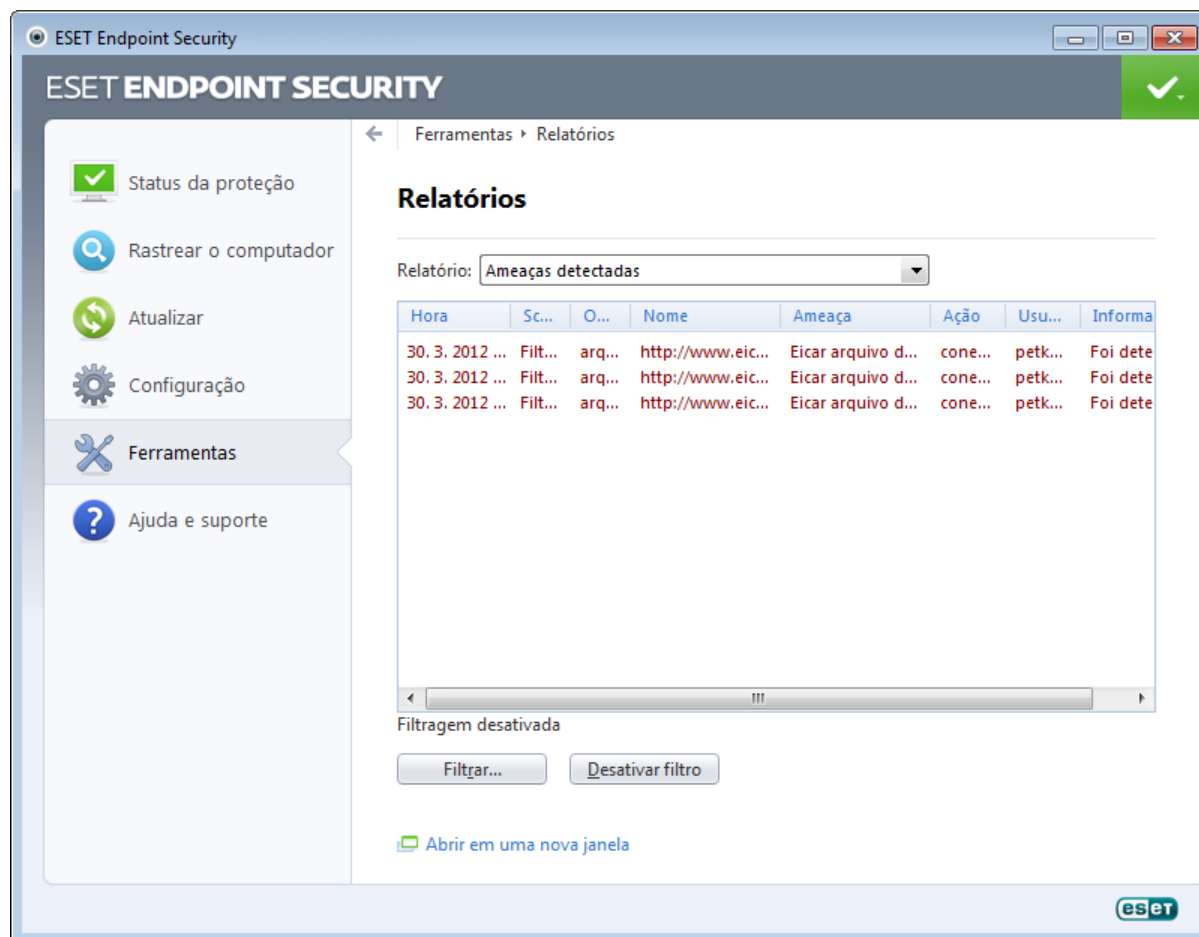
Esse menu inclui as seguintes ferramentas:

- Arquivos de log
- Estatísticas da proteção
- Monitorar atividade
- Processos em execução
- Agenda
- Quarentena
- Conexões de rede
- ESET SysInspector

**Enviar arquivo para análise** - Permite enviar um arquivo suspeito aos Laboratórios de vírus da ESET para análise. A janela de diálogo exibida depois de clicar nessa opção é descrita na seção Envio de arquivos para análise.

**ESET SysRescue** - Inicia o assistente de criação do ESET SysRescue.

### 4.6.1 Arquivos de log

Os arquivos de log contêm informações sobre todos os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detectadas. O registro em log atua como uma ferramenta essencial na análise do sistema, na detecção de ameaças e na solução de problemas. O registro em log realiza-se ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento do log. É possível visualizar mensagens de texto e logs diretamente do ambiente do ESET Endpoint Security, bem como arquivar logs.

Os arquivos de log podem ser acessados na janela principal do programa, clicando em **Ferramentas** > **Arquivos de log**. Selecione o tipo de log desejado no menu suspenso **Log** Os seguintes logs estão disponíveis:

- **Ameaças detectadas** - O log de ameaças fornece informações detalhadas sobre as infiltrações detectadas pelos módulos do ESET Endpoint Security. As informações incluem a hora da detecção, nome da ameaça, local, ação realizada e o nome do usuário conectado no momento em que a ameaça foi detectada. Clique duas vezes em qualquer entrada de log para exibir seus detalhes em uma janela separada.
- **Eventos** - Todas as ações importantes executadas pelo ESET Endpoint Security são registradas no log de eventos. O log de eventos contém informações sobre eventos e erros que ocorreram no programa. Essa opção foi desenvolvida para a solução de problemas de administradores do sistema e de usuários. Muitas vezes as informações encontradas aqui podem ajudá-lo a encontrar uma solução para um problema no programa.
- **Rastreamento do computador** - Os resultados de todos os rastreamentos concluídos são exibidos nessa janela. Cada linha corresponde a um rastreamento no computador. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo rastreamento.
- **HIPS** - Contém registros de regras específicas que foram marcadas para registro. O protocolo exibe o aplicativo que acionou a operação, o resultado (se a regra foi permitida ou proibida) e o nome da regra criada.
- **Firewall pessoal** - O log do firewall exibe todos os ataques remotos detectados pelo firewall pessoal. Aqui, você vai encontrar informações sobre todos os ataques em seu computador. A coluna Evento lista os ataques detectados. A coluna Origem informa mais sobre quem atacou. A coluna Protocolo revela o protocolo de comunicação usado para o ataque. A análise do log do firewall pode ajudá-lo a detectar tentativas de infiltração do sistema a tempo de evitar o acesso sem autorização ao sistema.

- **Proteção antispam** - Contém registros relacionados com emails marcados como spam.
- **Controle de Web** - Mostra endereços URL bloqueados ou permitidos e suas categorias. A coluna Ação executada mostra como as regras de filtragem foram aplicadas.
- **Controle de dispositivos** - Contém registros de dispositivos ou mídias removíveis que foram conectados ao computador. Apenas dispositivos com regra de controle de dispositivo respectiva serão registrados no arquivo de log. Se a regra não coincidir com um dispositivo conectado, uma entrada de log para um dispositivo conectado não será criada. Aqui, você também pode visualizar detalhes, como tipo de dispositivo, número de série, nome do fornecedor e tamanho da mídia (se disponível).

Em cada seção, as informações exibidas podem ser copiadas diretamente para a área de transferência (atalho do teclado: Ctrl + C), selecionando a entrada e clicando em **Copiar**. Para selecionar várias entradas, as teclas CTRL e SHIFT podem ser usadas.

Você pode exibir o menu de contexto clicando com o botão direito em um determinado registro. As seguintes opções também estão disponíveis no menu de contexto.

- **Filtrar registros do mesmo tipo** - Depois de ativar esse filtro, você só verá registros do mesmo tipo (diagnósticos, avisos...).
- **Filtrar.../Localizar...** - Depois de clicar nessa opção, uma janela chamada **Filtragem de logs** será aberta e você poderá definir os critérios de filtragem.
- **Desativar filtro** - Apaga todas as configurações do filtro (conforme descrição acima).
- **Copiar tudo** - Copia informações sobre todos os registros na janela.
- **Excluir/Excluir tudo** - Exclui o(s) registro(s) selecionado(s) ou todos os exibidos - essa ação requer privilégios de administrador.
- **Exportar** - Exporta informações sobre o(s) registro(s) em formato XML.
- **Percorrer log** - Deixe esta opção ativada para percorrer automaticamente logs antigos e monitorar logs ativos na janela **Arquivos de log**.

#### 4.6.1.1 Manutenção de logs

A configuração de arquivos de log do ESET Endpoint Security pode ser acessada na janela principal do programa. Clique em **Configuração** > **Entrar na configuração avançada...** > **Ferramentas** > **Arquivos de log**. A seção de arquivos de log é utilizada para definir como os logs serão gerenciados. O programa exclui automaticamente os logs mais antigos a fim de economizar espaço no disco rígido. Você pode especificar as seguintes opções para logs:

**Excluir automaticamente registros anteriores a (dias)** - As entradas de logs anteriores ao número de dias especificado são automaticamente excluídas.

**Otimizar automaticamente arquivos de log** - Se selecionada, os arquivos de log serão automaticamente desfragmentados se a porcentagem for superior ao valor especificado no campo **Se o número de registros não utilizados excede (%)**.

Clique em **Otimizar agora** para iniciar a desfragmentação dos arquivos de log. Todas as entradas de logs vazias são removidas durante esse processo, o que melhora o desempenho e a velocidade no processamento de logs. Essa melhoria pode ser observada especialmente se os logs tiverem um grande número de entradas.

**Detalhamento mínimo de registro em log** - Especifica o nível de detalhamento mínimo de eventos a serem registrados em log.

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, a firewall pessoal, etc...).

Clique em **Ativar protocolo de texto** para armazenar logs em outro formato de arquivo e fora de Arquivos de log:

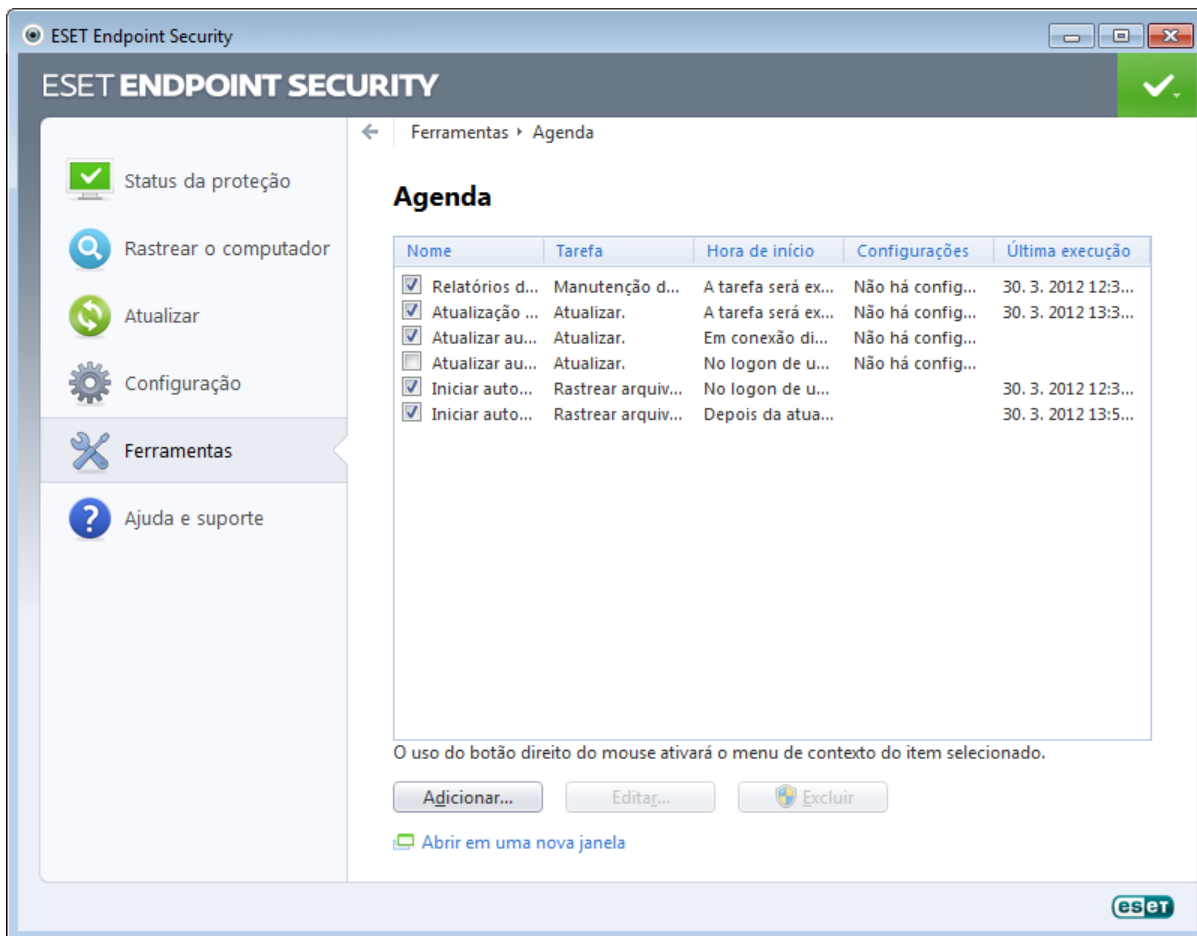
- **Tipo** - Se você escolher o formato de arquivo **Simples**, os logs serão armazenados em um arquivo texto; os dados serão separados por tabulações. O mesmo se aplica ao formato de arquivo **CSV** com separação por vírgulas. Se você escolher **Evento**, os logs serão armazenados no log de eventos do Windows (pode ser visualizado usando o Visualizador de Eventos no Painel de Controle) em oposição ao arquivo.
- **Diretório de destino** - Local onde os arquivos serão armazenados (aplica-se apenas a Simples/CSV). Cada seção de log tem seu próprio arquivo com nome de arquivo predefinido (p. ex., virlog.txt para a seção **Ameaças detectadas** de arquivos de log, se você usar formato de arquivo de texto simples para armazenar logs).

O botão **Excluir logs** apaga todos os logs armazenados que estão atualmente selecionados no menu suspenso **Tipo**.

### 4.6.2 Agenda

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas.

A Agenda pode ser acessada na janela principal do programa do ESET Endpoint Security em **Ferramentas** > **Agenda**. A **Agenda** contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

O Agendador serve para agendar as seguintes tarefas: atualização do banco de dados das assinaturas de vírus, tarefa de rastreamento, rastreamento de arquivos na inicialização do sistema e manutenção do log. Você pode adicionar ou excluir tarefas diretamente da janela principal da Agenda (clique em **Adicionar...** ou **Excluir** na parte inferior). Clique com o botão direito em qualquer parte na janela de Agenda para realizar as seguintes ações: exibir informações detalhadas, executar a tarefa imediatamente, adicionar uma nova tarefa e excluir uma tarefa existente. Use as caixas de seleção no início de cada entrada para ativar/desativar as tarefas.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Manutenção de logs**
- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**
- **Rastreamento de arquivos em execução durante inicialização do sistema** (após logon do usuário)
- **Verificação automática de arquivos durante inicialização do sistema** (após atualização bem sucedida do banco de dados de assinatura de vírus)

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificar e clique no botão **Editar...**.

#### Adicionar uma nova tarefa

1. Clique em **Adicionar...** na parte inferior da janela.

2. Selecione a tarefa desejada no menu suspenso.

Adicionar tarefa

Tarefa agendada:

Executar aplicativo externo

Executar aplicativo externo
Manutenção dos relatórios
Rastrear arquivos na inicialização do sistema
Criar um snapshot do status do computador
Rastreamento sob demanda do computador
Atualizar
Verificando se há uma versão mais recente do produto

Mais informações sobre o agendamento de tarefa...

< Voltar | Avançar > | Cancelar

3. Insira o nome da tarefa e selecione uma das seguintes opções de tempo:
    - **Uma vez** - A tarefa será realizada somente uma vez, na data e hora predefinidas.
    - **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado (em horas).
    - **Diariamente** - A tarefa será realizada diariamente na hora especificada.
    - **Semanalmente** - A tarefa será realizada uma ou mais vezes por semana, no(s) dia(s) e hora selecionados.
    - **Evento disparado** - A tarefa será realizada após um evento especificado.

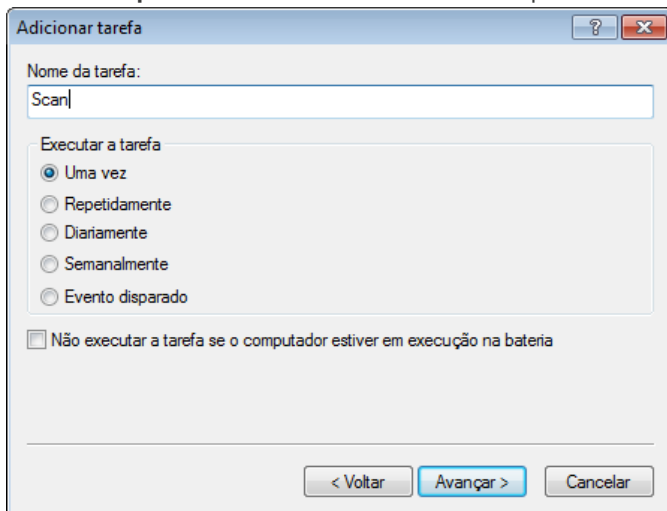
Adicionar tarefa

Nome da tarefa:

Scan

Executar a tarefa
Uma vez
Repetidamente
Diariamente
Semanalmente
Evento disparado

Não executar a tarefa se o computador estiver em execução na bateria

< Voltar | Avançar > | Cancelar

4. Dependendo da opção de tempo escolhida na etapa anterior, uma destas janelas de diálogo será exibida:
    - **Uma vez** - A tarefa será realizada na data e hora predefinidas.
    - **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado.
    - **Diariamente** - A tarefa será executada repetidamente todos os dias no horário especificado.
    - **Semanalmente** - A tarefa será realizada na data e hora selecionadas.
5. Se não foi possível executar a tarefa em um horário predefinido, você pode especificar quando ela será executada novamente:
    - Aguardar até a próxima hora agendada
    - Executar a tarefa tão logo quanto possível
    - Executar a tarefa imediatamente se o período de tempo desde a última execução da tarefa for maior que -- horas
6. Na última etapa, você pode revisar a tarefa agendada. Clique em **Concluir** para aplicar a tarefa.

Editar tarefa

A tarefa foi agendada.

Visão geral da tarefa agendada

**Nome da tarefa:**
Atualizar automaticamente após conexão dial-up

**Tipo de tarefa:**
Atualizar.

**Executar tarefa:**
Em conexão dial-up com a Internet/VPN (uma vez por hora no máximo).

**Ação a ser realizada se a tarefa não for executada na hora especificada:**
A tarefa não será executada.

Executar a tarefa com parâmetros específicos

< Voltar | Finalizar | Cancelar

#### 4.6.2.1 Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique no botão **Adicionar...** ou clique com o botão direito do mouse e selecione **Adicionar...** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo externo** - Agenda a execução de um aplicativo externo.
- **Manutenção de logs** - Os arquivos de log também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos arquivos de log para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que estão permitidos para serem executados no logon ou na inicialização do sistema.
- **Criar um snapshot do status do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastreamento do computador** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Atualizar** - Agenda uma tarefa de atualização, atualizando o banco de dados de assinatura de vírus e os módulos do programa.

Como **Atualizar** é uma das tarefas agendadas usadas com mais frequência, explicaremos a seguir como adicionar uma nova tarefa de atualização.

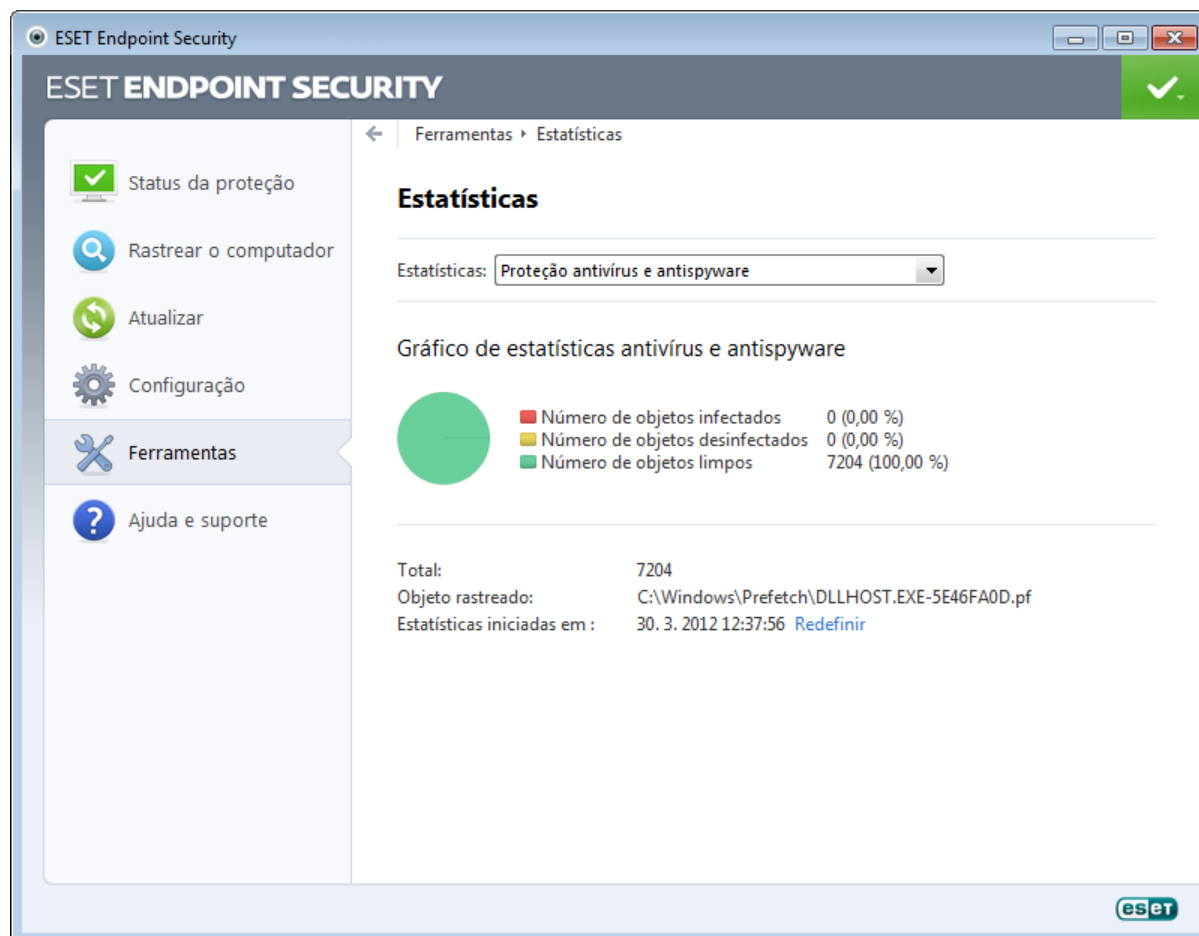
No menu suspenso **Tarefa agendada**, selecione **Atualizar**. Clique em **Avançar** e insira o nome da tarefa no campo **Nome da tarefa**. Selecione a frequência da tarefa. As opções disponíveis são: **Uma vez**, **Repetidamente**, **Diariamente**, **Semanalmente** e **Evento disparado**. Use a opção **Não executar a tarefa se o computador estiver em execução na bateria** para minimizar os recursos do sistema enquanto o laptop estiver em execução na bateria. Com base na frequência selecionada, diferentes parâmetros de atualização serão exibidos para você. Depois defina a ação a ser tomada se a tarefa não puder ser executada ou concluída na hora agendada. As três opções a seguir estão disponíveis:

- **Aguardar até a próxima hora agendada**
- **Executar a tarefa tão logo quanto possível**
- **Executar a tarefa imediatamente se a hora desde a última execução exceder o intervalo especificado** (o intervalo pode ser definido utilizando a caixa de rolagem Intervalo da tarefa)

Na próxima etapa, uma janela de resumo com informações sobre a tarefa agendada atual é exibida; a opção **Executar a tarefa com parâmetros específicos** deve ser ativada automaticamente. Clique no botão **Concluir**.

Uma janela de diálogo será exibida permitindo selecionar perfis a serem utilizados para a tarefa agendada. Aqui é possível especificar um perfil primário e um alternativo, que será usado caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em **OK** na janela **Atualizar perfis**. A nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

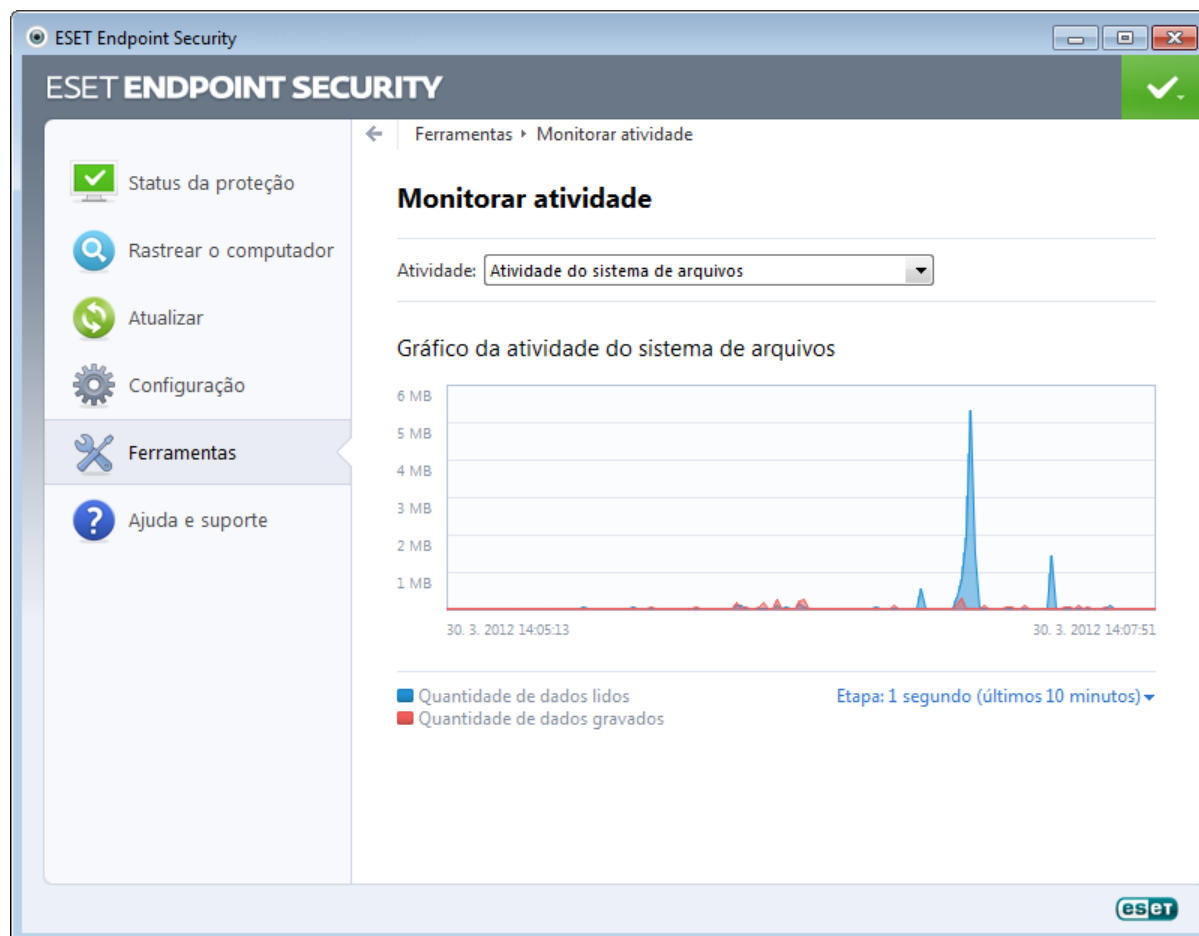
### 4.6.3 Estatísticas da proteção

Para exibir um gráfico de dados estatísticos relacionados aos módulos de proteção do ESET Endpoint Security, clique em **Ferramentas** > **Estatísticas da proteção**. Selecione o módulo de proteção desejado no menu suspenso **Estatísticas** para visualizar o gráfico e a legenda correspondentes. Se você passar o mouse sobre um item na legenda, somente os dados desse item serão exibidos no gráfico.

Os gráficos estatísticos a seguir estão disponíveis:

- **Proteção antifírus e antispyware** - Exibe o número de objetos infectados e limpos.
- **Proteção em tempo real do sistema de arquivos** - Exibe apenas os objetos que foram lidos ou gravados no sistema de arquivos.
- **Proteção do cliente de email** - Exibe apenas os objetos que foram enviados ou recebidos pelos clientes de email.
- **Proteção do acesso à web** - Exibe apenas os objetos obtidos por download pelos navegadores da Web.
- **Proteção antispam do cliente de email** - Exibe o histórico das estatísticas de antispam desde a última inicialização.

Abaixo dos gráficos de estatísticas, você pode ver o número total de objetos rastreados, o último objeto rastreado e o registro de estatísticas. Clique em **Redefinir** para apagar todas as informações estatísticas.

### 4.6.4 Monitorar atividade

Para visualizar a **Atividade do sistema de arquivos** atual em forma gráfica, clique em **Ferramentas** > **Monitorar atividade**. Na parte inferior do gráfico, há uma linha do tempo que grava a atividade do sistema de arquivos em tempo real com base na duração do tempo selecionado. Para alterar a duração do tempo, clique em **Etapa 1...** no canto inferior direito da janela.

As opções disponíveis são:

- **Etapa: 1 segundo (últimos 10 minutos)** - O gráfico é atualizado a cada segundo e a linha de tempo cobre os últimos 10 minutos
- **Etapa: 1 minuto (últimas 24 horas)** - O gráfico é atualizado a cada minuto e a linha de tempo cobre as últimas 24 horas
- **Etapa: 1 hora (último mês)** - O gráfico é atualizado a cada hora e a linha de tempo cobre o último mês
- **Etapa: 1 hora (mês selecionado)** - O gráfico é atualizado a cada hora e a linha de tempo cobre os últimos X meses selecionados

O eixo vertical do **Gráfico da atividade do sistema de arquivos** representa os dados lidos (azul) e os dados gravados (vermelho). Ambos os valores são fornecidos em KB (kilobytes)/MB/GB. Se você passar o mouse sobre os dados lidos ou sobre os dados gravados na legenda embaixo do gráfico, apenas os dados para esse tipo de atividade serão exibidos no gráfico.

Também é possível selecionar exibir a **Atividade de rede** no menu suspenso **Atividade**. A exibição do gráfico e as opções da **Atividade do sistema de arquivos** e da **Atividade de rede** são as mesmas, exceto que a última exibe os dados recebidos (azul) e os dados enviados (vermelho).

### 4.6.5 ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o computador, coleta informações detalhadas sobre os componentes do sistema, como os drivers e aplicativos instalados, as conexões de rede ou entradas de registo importantes, e avalia o nível de risco de cada componente. Essas informações podem ajudar a determinar a causa do comportamento suspeito do sistema, que pode ser devido a incompatibilidade de software ou hardware ou infecção por malware.

A janela do SysInspector exibe as seguintes informações sobre os logs criados:

- **Hora** - A hora de criação do log.
- **Comentário** - Um comentário curto.
- **Usuário** - O nome do usuário que criou o log.
- **Status** - O status de criação do log.

As seguintes ações estão disponíveis:

- **Comparar** - Compara dois logs existentes.
- **Criar...** - Cria um novo log. Aguarde até que o log do ESET SysInspector seja concluído (**Status** exibido como Criado).
- **Excluir** - Remove os logs selecionados da lista.

Após clicar com o botão direito em um ou mais logs selecionados, as seguintes opções estarão disponíveis no menu de contexto:

- **Mostrar** - Abre o log selecionado no ESET SysInspector (igual a clicar duas vezes em um log).
- **Excluir tudo** - Exclui todos os logs.
- **Exportar...** - Exporta o log para um arquivo .xml ou .xml compactado.

### 4.6.6 ESET Live Grid

O ESET Live Grid (a próxima geração do ThreatSense.Net) é um sistema de avisos avançado contra ameaças emergentes com base na reputação. Usando a transmissão contínua em tempo real de informações relacionadas a ameaças da nuvem, o laboratório de vírus da ESET mantém as defesas atualizadas para oferecer um nível de proteção constante. O usuário pode verificar a reputação dos arquivos e dos processos em execução diretamente da interface do programa ou no menu de contexto, com informações adicionais disponíveis no ESET Live Grid. Há duas opções:

1. Você decide se deseja ou não ativar o ESET Live Grid. Você não perderá nenhuma funcionalidade do software e ainda receberá a melhor proteção que oferecemos.
2. É possível configurar o ESET Live Grid para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido. Esse arquivo pode ser enviado para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar suas capacidades de detecção de ameaças.

O ESET Live Grid coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Por padrão, o ESET Endpoint Security é configurado enviar arquivos suspeitos ao Laboratório de vírus da ESET para análise detalhada. Os arquivos com certas extensões, como .doc ou .xls, são sempre excluídos. Você também pode adicionar outras extensões se houver arquivos específicos cujo envio você ou sua empresa desejam impedir.

O menu de configuração do ESET Live Grid fornece várias opções para ativar/desativar o ESET Live Grid, que serve para enviar arquivos suspeitos e informações estatísticas anônimas para os laboratórios da ESET. Ele pode ser acessado a partir da árvore Configuração avançada clicando em **Ferramentas** > **ESET Live Grid**.

**Participar do ESET Live Grid** - Ativa/desativa o ESET Live Grid, que serve para enviar arquivos suspeitos e informações estatísticas anônimas para os laboratórios da ESET.

**Não enviar estatísticas** – Selecione essa opção se você não quiser enviar informações anônimas a partir do ESET Live Grid sobre seu computador. Essas informações estão relacionadas às ameaças detectadas recentemente que podem incluir o nome da infiltração, informação sobre a data e hora em que ela foi detectada, a versão do ESET Endpoint Security, informações sobre o sistema operacional do computador e as configurações de Local. As estatísticas são geralmente entregues ao servidor da ESET uma ou duas vezes ao dia.

**Não enviar arquivos** – Arquivos suspeitos, que se pareçam com infiltrações em seus conteúdos ou comportamento, não são enviados à ESET para análise por meio da tecnologia ESET Live Grid.

**Configuração avançada...** - Abre uma janela com configurações adicionais do ESET Live Grid .

Se já tiver usado o ESET Live Grid antes e o tiver desativado, ainda pode haver pacotes de dados a enviar. Mesmo depois da desativação, tais pacotes serão enviados à ESET na próxima ocasião. Posteriormente, não serão criados pacotes adicionais.

#### 4.6.6.1 Arquivos suspeitos

A guia **Arquivos** da configuração avançada do ESET Live Grid permite configurar como as ameaças serão enviadas ao Laboratório de vírus da ESET para análise.

Se encontrar um arquivo suspeito, você poderá enviá-lo para análise no nosso Laboratório de ameaças. Se for um aplicativo malicioso, sua detecção será adicionada à próxima atualização de assinaturas de vírus.

**Filtro de exclusões** - O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Os arquivos relacionados nunca serão enviados aos laboratórios da ESET para análise, mesmo se incluírem um código suspeito. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.

**Email de contato (opcional)** - Seu email de contato pode ser incluído com qualquer arquivo suspeito e ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

Nesta seção, é possível escolher quais arquivos e informações estatísticas serão enviadas através do administrador remoto da ESET ou diretamente para à ESET. Se deseja garantir que os arquivos suspeitos e as informações estatísticas foram entregues à ESET, selecione a opção **Através do Administrador Remoto ou diretamente para à ESET**. Neste caso, os arquivos e as estatísticas são enviados por todos os meios disponíveis. O envio de arquivos suspeitos através do administrador remoto envia arquivos e estatísticas para o servidor de administração remota, o que garante o envio subsequente aos laboratórios de análise de vírus da ESET. Se a opção **Diretamente para à ESET** estiver selecionada, todos os arquivos suspeitos e as informações estatísticas serão enviados ao laboratório de análise de vírus da ESET a partir do programa.

Selecione a opção **Ativar registro em log** para criar um log de eventos para registrar os envios de arquivos e informações estatísticas. Ela permite o registro no Log de eventos quando arquivos ou estatísticas são enviados.

### 4.6.7 Processos em execução

Os processos em execução exibem os programas ou processos em execução no computador e mantêm a ESET imediatamente e continuamente informada sobre novas infiltrações. O ESET Endpoint Security oferece informações detalhadas sobre os processos em execução a fim de proteger os usuários com a tecnologia ESET Live Grid.

ESET Endpoint Security

ESET ENDPOINT SECURITY

Status da proteção
Rastrear o computador
Atualizar
Configuração
Ferramentas
Ajuda e suporte

Ferramentas ▸ Processos em execução

**Processos em execução**

Esta janela exibe uma lista de processos em execução com informações adicionais no ESET Live Grid. O nível de risco de cada um é indicado, juntamente com o número de usuários e a hora da primeira descoberta.

| Processo | Níve... | Númer... | Hora da de... | Nome do aplica... |
| --- | --- | --- | --- | --- |
| smss.exe | | | dois anos atrás | Microsoft® Windo... |
| csrss.exe | | | dois anos atrás | Microsoft® Windo... |
| wininit.exe | | | dois anos atrás | Microsoft® Windo... |
| winlogon.exe | | | dois anos atrás | Microsoft® Windo... |
| services.exe | | | dois anos atrás | Microsoft® Windo... |
| lsass.exe | | | um mês atrás | Microsoft® Windo... |
| lsm.exe | | | dois anos atrás | Microsoft® Windo... |
| svchost.exe | | | dois anos atrás | Microsoft® Windo... |
| vboxservice.exe | | | três meses atrás | Oracle VM VirtualB... |
| spoolsv.exe | | | um ano atrás | Microsoft® Windo... |
| taskhost.exe | | | dois anos atrás | Microsoft® Windo... |

**Arquivo:** c:\windows\system32\lsass.exe
**Tamanho do arquivo:** 22.0 kB
**Descrição do arquivo:** Local Security Authority Process
**Nome da empresa:** Microsoft Corporation
**Versão do arquivo:** 6.1.7600.16915 (win7_gdr.111116-1506)
**Nome do produto:** Microsoft® Windows® Operating System

Abrir em uma nova janela

eset

**Processo** - Nome da imagem do programa ou processo em execução no computador. Você também pode usar o Gerenciador de tarefas do Windows para ver todos os processos que estão em execução no computador. O Gerenciador de tarefas pode ser aberto clicando-se com o botão direito em uma área vazia da barra de tarefas e, em seguida, clicando na opção Gerenciador de tarefas ou pressionando Ctrl+Shift+Esc no teclado.

**Nível de risco** - Na maioria dos casos, o ESET Endpoint Security e a tecnologia ESET Live Grid atribui níveis de risco aos objetos (arquivos, processos, chaves de registro etc.), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 - Aceitável (verde) a 9 - Perigoso (vermelho).

**OBSERVAÇÃO:** Aplicativos conhecidos marcados como Aceitável (verde) são limpos definitivamente (lista de permissões) e serão excluídos do rastreamento, pois isso melhorará a velocidade do rastreamento sob demanda do computador ou da Proteção em tempo real do sistema de arquivos no computador.

**Número de usuários** - O número de usuários que utilizam um determinado aplicativo. Estas informações são reunidas pela tecnologia ESET Live Grid.

**Hora da descoberta** - Período de tempo a partir do momento em que o aplicativo foi detectado pela tecnologia ESET Live Grid.

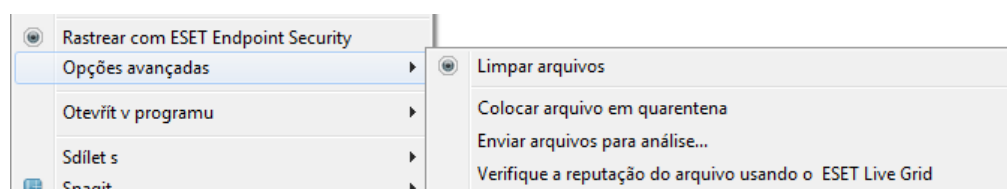
**OBSERVAÇÃO:** Quando um aplicativo é marcado com o nível de segurança Desconhecido (laranja), não é necessariamente um software malicioso. Geralmente, é apenas um aplicativo mais recente. Se não tiver certeza sobre o arquivo, você poderá enviar o arquivo para análise ao Laboratório de Vírus da ESET. Se for detectado que o arquivo é um aplicativo malicioso, sua detecção será adicionada em uma das atualizações posteriores.

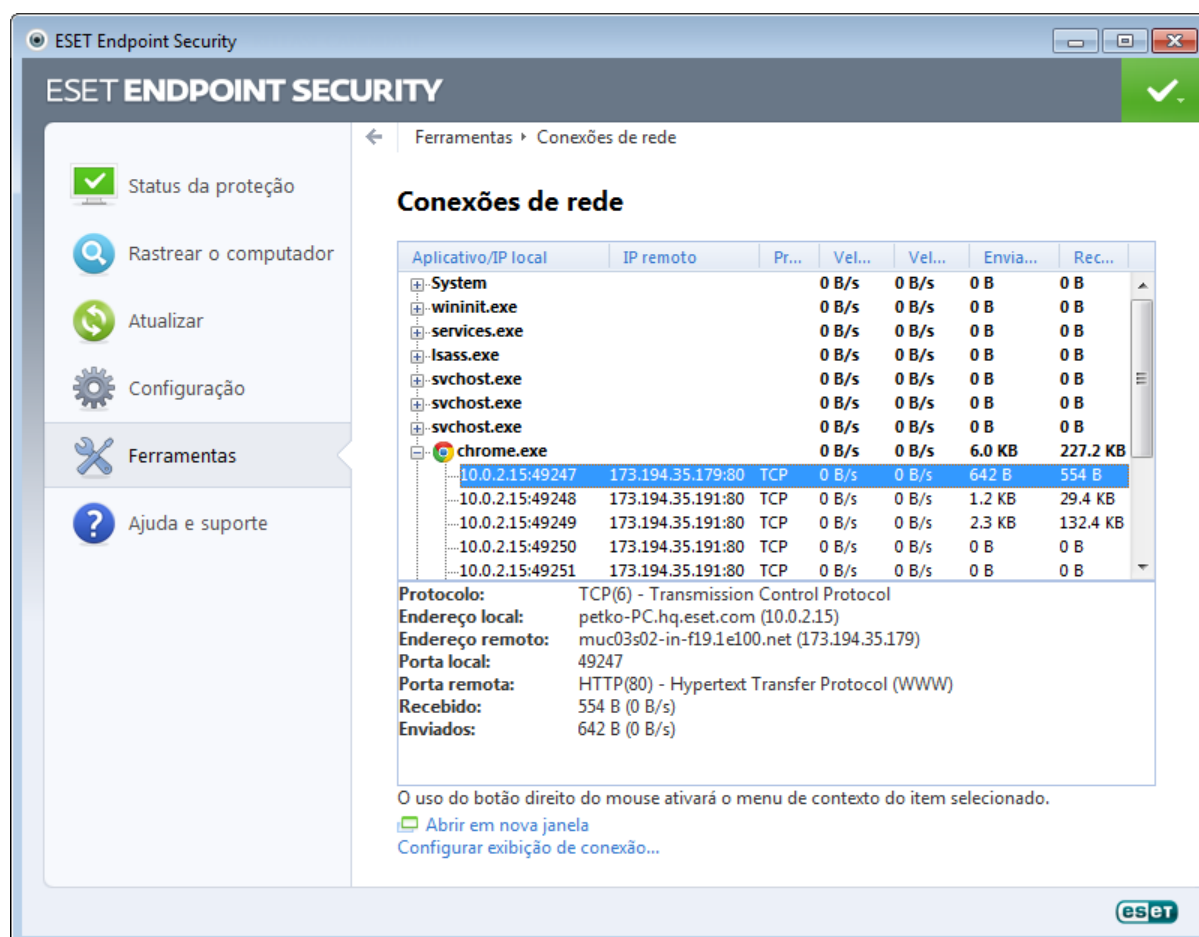
**Nome do aplicativo** - O nome de um programa ou processo.

**Abrir em uma nova janela** - As informações dos processos em execução serão abertas em uma nova janela.

Ao clicar em um determinado aplicativo na parte inferior, as seguintes informações serão exibidas na parte inferior da janela:

- **Arquivo** - Local de um aplicativo no computador.
- **Tamanho do arquivo** - Tamanho do arquivo em kB (kilobytes) ou MB (megabytes).
- **Descrição do arquivo** - Características do arquivo com base na descrição do sistema operacional.
- **Nome da empresa** - Nome de processo do aplicativo ou do fornecedor.
- **Versão do arquivo** - Informações do editor do aplicativo.
- **Nome do produto** - Nome do aplicativo e/ou nome comercial.

**OBSERVAÇÃO:** A reputação também pode ser verificada em arquivos que não agem como programas/processos em execução - marque os arquivos que deseja verificar, clique neles com o botão direito do mouse e, no menu de contexto, selecione **Opções avançadas** > **Verificar reputação do arquivo usando o ESET Live Grid**.

### 4.6.8 Conexões de rede

Na seção Conexões de rede, você pode ver uma lista de conexões ativas e pendentes. Isso o ajuda a controlar todos os aplicativos que estabelecem conexões de saída.

A primeira linha exibe o nome do aplicativo e a velocidade de transferência dos dados. Para ver a lista de conexões feitas pelo aplicativo (bem como informações mais detalhadas), clique em **+**.

**Aplicativo/IP local** - Nome do aplicativo, endereços IP locais e portas de comunicação.

**IP remoto** - Endereço IP e número de porta de um computador remoto específico.

**Protocolo** - Protocolo de transferência usado.

**Velocidade de entrada/de saída** - A velocidade atual dos dados de saída e entrada.

**Enviados/Recebidos** - Quantidade de dados trocados na conexão.

**Abrir em uma nova janela** - Exibe as informações em uma janela separada.

A opção **Configuração de visualização da conexão...** na tela Conexões de rede insere a estrutura de configuração avançada para esta seção, permitindo a modificação das opções de exibição da conexão:

**Solucionar nomes de host** - Se possível, todos os endereços de rede serão exibidos no formato DNS, não no formato de endereço IP numérico.

**Somente conexões de protocolo TCP** - A lista só exibe conexões que pertencem ao pacote de protocolo TCP.

**Mostrar conexões com portas abertas nas quais o computador está na escuta** - Selecione essa opção para exibir somente conexões em que não haja comunicação atualmente estabelecida, mas o sistema tenha aberto uma porta e esteja aguardando por conexão.

**Mostrar também conexões no computador** - Selecione essa opção para mostrar somente conexões nas quais o lado remoto é um sistema local - as chamadas conexões de localhost.

Clique com o botão direito do mouse em uma conexão para visualizar as opções adicionais, que incluem:

**Negar comunicação para a conexão** - Encerra a comunicação estabelecida. Essa opção só fica disponível depois que você clica em uma conexão ativa.

**Mostrar detalhes** - Escolha esta opção para exibir informações detalhadas sobre a conexão selecionada.

**Velocidade de atualização** – Escolha a frequência para atualizar as conexões ativas.

**Atualizar agora** - Recarrega a janela Conexões de rede.

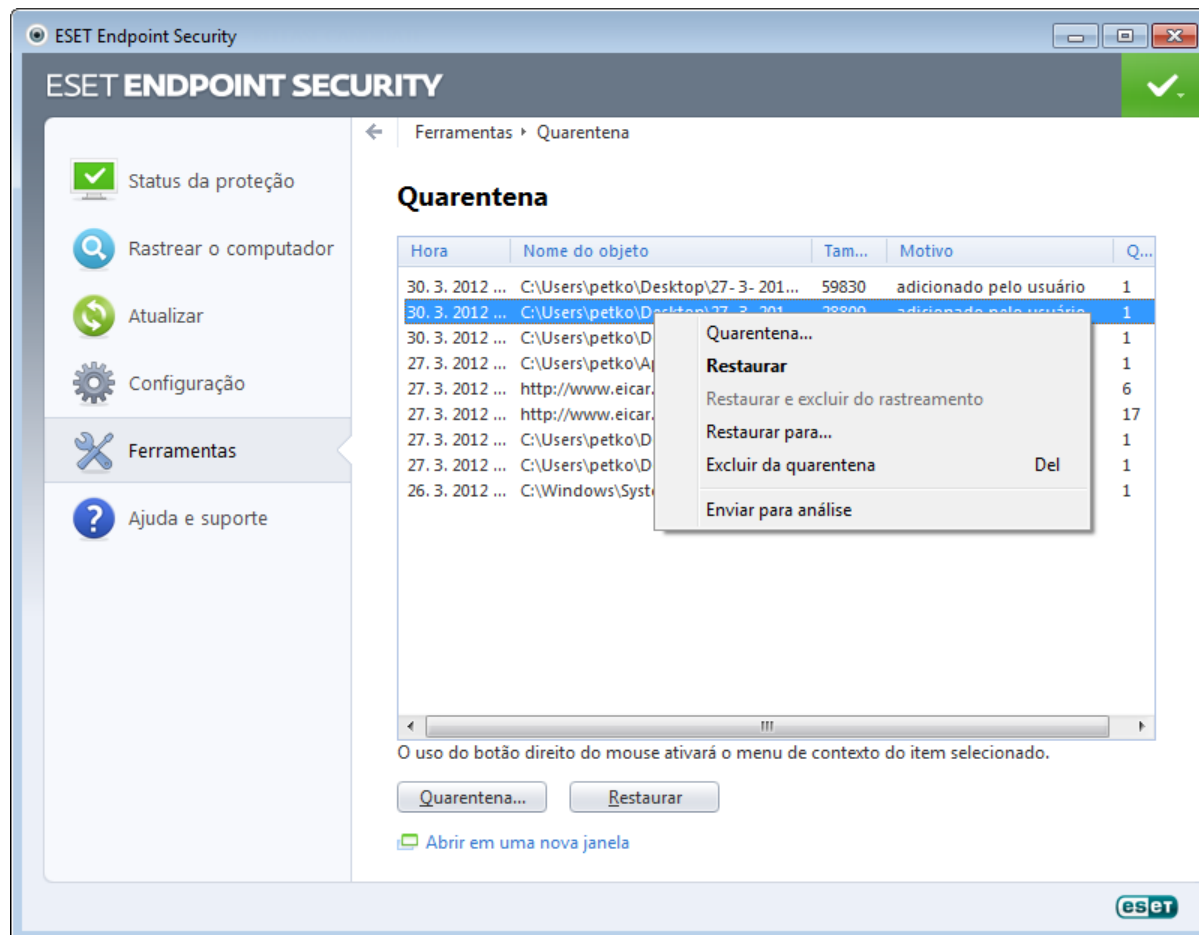
As opções a seguir só ficam disponíveis depois que você clica em um aplicativo ou processo, não em uma conexão ativa:

**Negar temporariamente comunicação para o processo** - Rejeita as atuais conexões de determinado aplicativo. Se uma nova conexão for estabelecida, o firewall utilizará uma regra predefinida. Uma descrição das configurações pode ser encontrada na seção Regras e zonas.

**Permitir temporariamente comunicação para o processo** - Permite as conexões atuais de determinado aplicativo. Se uma nova conexão for estabelecida, o firewall utilizará uma regra predefinida. Uma descrição das configurações pode ser encontrada na seção Regras e zonas.

### 4.6.9 Quarentena

A principal função da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Endpoint Security.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo rastreador de antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de vírus da ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (por exemplo, objeto adicionado pelo usuário) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas ameaças).

#### Colocação de arquivos em quarentena

O ESET Endpoint Security coloca automaticamente os arquivos excluídos em quarentena (se você não cancelou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando em **Quarentena...**. Se este for o caso, o arquivo original não será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela **Quarentena** e selecione **Quarentena...**

#### Restauração da Quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Utilize o recurso **Restaurar** para essa finalidade, que está disponível no menu de contexto clicando com o botão direito do mouse no arquivo desejado, na janela Quarentena. Se um arquivo for marcado como um Aplicativo potencialmente não desejado, a opção **Restaurar e excluir do rastreamento** será ativada. Leia mais sobre esse tipo de aplicativo no glossário. O menu de contexto oferece também a opção **Restaurar para...**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

**OBSERVAÇÃO**: se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do rastreamento após restaurá-lo e envie-o para o Atendimento ao Cliente da ESET.

#### Envio de um arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi determinado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de vírus da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

### 4.6.10 Envio de arquivos para análise

A caixa de diálogo de envio de arquivos permite enviar um arquivo para a ESET para fins de análise e pode ser acessada em **Ferramentas** > **Enviar arquivo para análise**. Se você detectar um arquivo com comportamento suspeito no seu computador, poderá enviá-lo para o Laboratório de vírus da ESET para análise. Se for detectado que o arquivo é um aplicativo malicioso, sua detecção será adicionada em uma das atualizações posteriores.

Como alternativa, você pode enviar o arquivo por email. Se for esta sua opção, compacte o(s) arquivo(s) usando WinRAR/ZIP, proteja o arquivo com a senha "infected" (infectado) e envie-o para samples@eset.com. Lembre-se de incluir uma linha de assunto clara e o máximo de informações possível sobre o arquivo (por exemplo, o site do qual fez o download).

**OBSERVAÇÃO:** Antes de enviar um arquivo para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:
- o arquivo não foi detectado,
- o arquivo foi detectado incorretamente como uma ameaça.

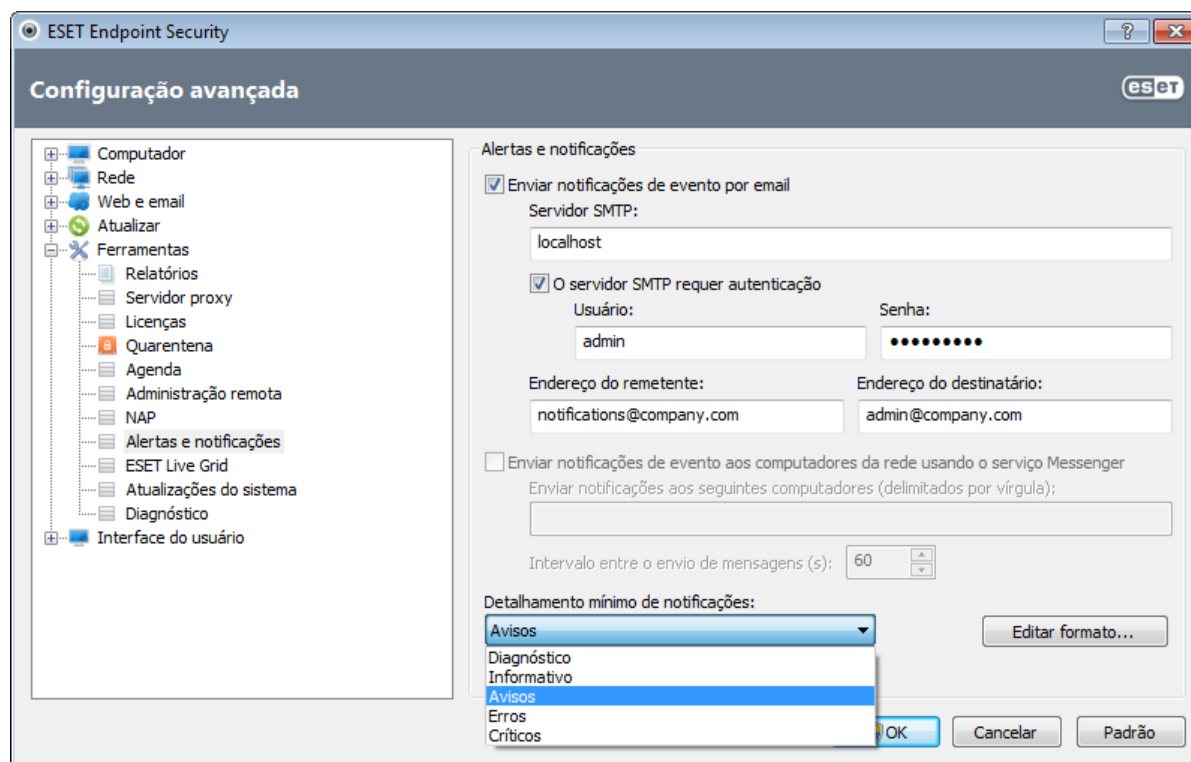
Você não receberá uma resposta, a não ser que mais informações sejam necessárias para a análise.

Selecione a descrição no menu suspenso **Motivo para envio do arquivo** mais adequada à sua mensagem:
- **Arquivo suspeito**,
- **Falso positivo** (arquivo que é detectado como uma infecção, mas que não está infectado),
- e **Outros**.

**Arquivo** - O caminho do arquivo que você pretende enviar.

**Email de contato** - O email de contato é enviado junto com arquivos suspeitos para a ESET e pode ser utilizado para contatar você se informações adicionais sobre os arquivos suspeitos forem necessárias para análise. É opcional inserir um email de contato. Você não obterá uma resposta da ESET, a menos que mais informações sejam necessárias, pois a cada dia os nossos servidores recebem milhares de arquivos, o que torna impossível responder a todos os envios.

### 4.6.11 Alertas e notificações

O ESET Endpoint Security suportará o envio de emails se um evento com o nível de detalhamento selecionado ocorrer. Clique na caixa de seleção **Enviar notificações de evento por email** para ativar este recurso e ativar as notificações por e-mail.

**Servidor SMTP** - O servidor SMTP usado para o envio de notificações.

**Observação:** Os servidores SMTP com criptografia SSL/TLS não são suportados pelo ESET Endpoint Security.

**O servidor SMTP requer autenticação** - Se o servidor SMTP exigir autenticação, esses campos devem ser preenchidos com nome de usuário e senha válidos, concedendo acesso ao servidor SMTP.

**Endereço do remetente** - Esse campo especifica o endereço do remetente que será exibido no cabeçalho dos emails de notificação.

**Endereço do destinatário** - Esse campo especifica o endereço do destinatário que será exibido no cabeçalho dos emails de notificação.

**Enviar notificações de evento aos computadores da rede usando o serviço Messenger** - Marque esta caixa de seleção para enviar mensagens para computadores na rede local por meio do serviço de mensagem do Windows®.

**Enviar notificações aos seguintes computadores (delimitados por vírgula)** - Insira os nomes dos computadores que receberão notificações por meio do serviço de mensagens do Windows®.

**Intervalo entre o envio de mensagens (s)** - Para alterar a duração do intervalo entre notificações enviadas por meio da rede local, digite o intervalo de tempo desejado em segundos.

**Detalhamento mínimo de notificações** - Especifica o nível de detalhamento mínimo de notificações a serem enviadas.

**Editar formato...** - As comunicações entre o programa e um usuário remoto ou administrador do sistema são feitas por meio de emails ou mensagens de rede local (usando o serviço de mensagens do Windows®). O formato padrão das mensagens de alerta e notificações será o ideal para a maioria das situações. Em algumas circunstâncias, você pode precisar alterar o formato da mensagem - clique em Editar formato....

### 4.6.11.1 Formato de mensagem

Aqui é possível configurar o formato das mensagens de eventos que são exibidas em computadores remotos.

As mensagens de alerta e notificação de ameaças têm um formato padrão predefinido. Não aconselhamos alterar esse formato. No entanto, em algumas circunstâncias (por exemplo, se você tiver um sistema de processamento de email automatizado), você pode precisar alterar o formato da mensagem.

As palavras-chave (cadeias de caractere separadas por sinais %) são substituídas na mensagem pelas informações reais conforme especificadas. As palavras-chave disponíveis são:

- **%TimeStamp%** - Data e hora do evento.
- **%Scanner%** - Módulo relacionado.
- **%ComputerName%** - Nome do computador no qual o alerta ocorreu.
- **%ProgramName%** - Programa que gerou o alerta.
- **%InfectedObject%** - Nome do arquivo e mensagem infectados etc.
- **%VirusName%** - Identificação da infecção.
- **%ErrorDescription%** - Descrição de um evento não vírus.

As palavras-chave **%InfectedObject%** e **%VirusName%** são usadas somente em mensagens de alerta de ameaça, enquanto **%ErrorDescription%** é usada somente em mensagens de evento.

**Utilizar caracteres do alfabeto local** - Converte uma mensagem de email para a codificação de caracteres ANSI com base nas configurações regionais do Windows (por exemplo, windows-1250). Se você deixar essa opção desmarcada, uma mensagem será convertida e codificada em ACSII de 7 bits (por exemplo, "á" será alterada para "a" e um símbolo desconhecido para "?").

**Utilizar codificações de caracteres locais** - A origem da mensagem de email será codificada para o formato Quoted-printable (QP) que usa caracteres ASCII e pode transmitir caracteres nacionais especiais por email no formato de 8 bits (áéíóú).

## 4.6.12 Atualizações do sistema

O recurso de atualização do Windows é um componente importante de proteção de usuários contra software malicioso. Por esse motivo, é extremamente importante manter as atualizações do Microsoft Windows em dia, instalando-as assim que forem disponibilizadas. O ESET Endpoint Security o notificará sobre as atualizações ausentes de acordo com o nível que você especificar. Os seguintes níveis estão disponíveis:

- **Nenhuma atualização** - Nenhuma atualização de sistema será proposta para download.
- **Atualizações opcionais** - Atualizações marcadas como de baixa prioridade e superiores serão propostas para download.
- **Atualizações recomendadas** - Atualizações marcadas como comuns e superiores serão propostas para download.
- **Atualizações importantes** - Atualizações marcadas como importantes e superiores serão propostas para download.
- **Atualizações críticas** - Apenas atualizações críticas serão propostas para download.

Clique em **OK** para salvar as alterações. A janela Atualizações do sistema será exibida depois da verificação do status com o servidor de atualização. Assim, as informações sobre atualização de sistema podem não estar disponíveis imediatamente após as alterações serem salvas.

## 4.6.13 Diagnóstico

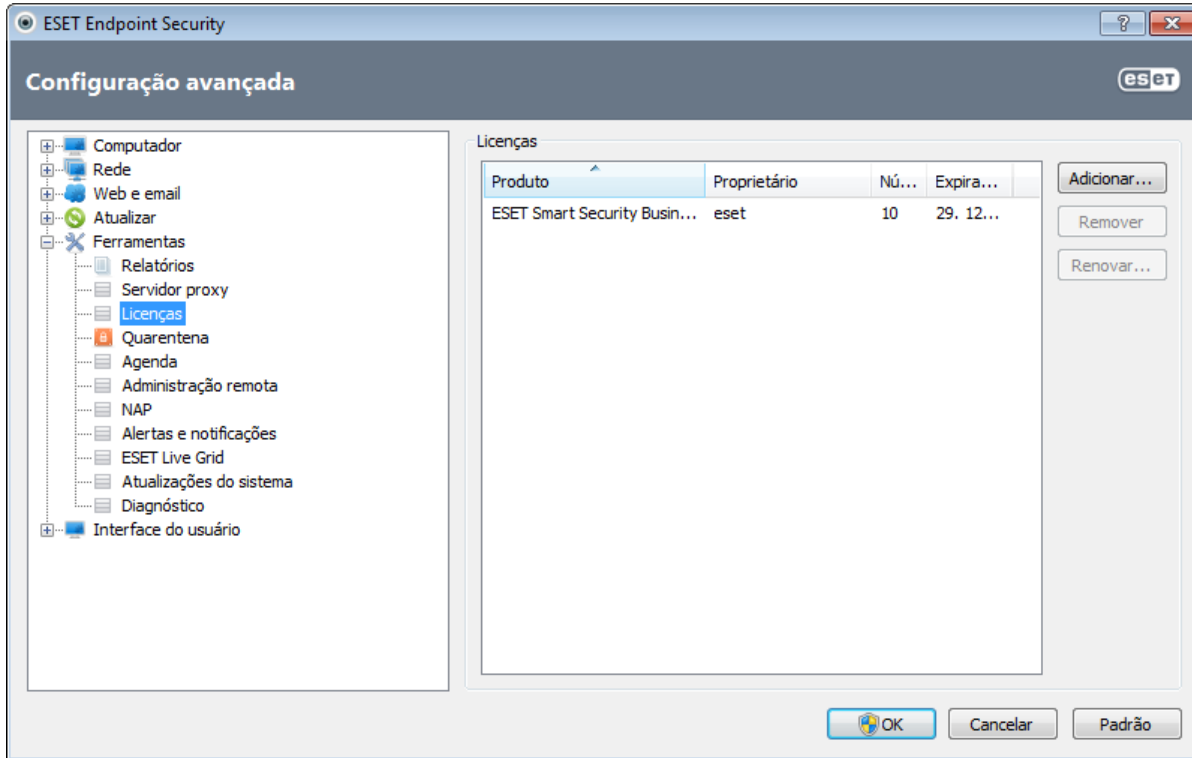
O diagnóstico fornece despejos de memória de aplicativos dos processos da ESET (por exemplo, ekrn). Se um aplicativo falhar, um despejo será gerado. Isso poderá ajudar os desenvolvedores a depurar e a corrigir os problemas do ESET Endpoint Security. Estão disponíveis dois tipos de despejos:

- **Despejo de memória completo** - Registra todo o conteúdo da memória do sistema quando o aplicativo pára inesperadamente. Um despejo de memória completo pode conter dados de processos que estavam em execução quando o despejo de memória foi coletado.
- **Despejo de memória resumido** - Registra o menor conjunto de informações úteis que podem ajudar a identificar porque o aplicativo parou inesperadamente. Esse tipo de arquivo de despejo pode ser útil quando o espaço é limitado. No entanto, devido às informações limitadas incluídas, os erros que não foram causados diretamente pelo encadeamento que estava em execução no momento em que o problema ocorreu, podem não ser descobertos por uma análise desse arquivo.
- Selecione **Não gerar despejo de memória** (padrão) para desativar esse recurso.

**Diretório de destino** – Diretório no qual o despejo durante a falha será gerado. Clique em **Abrir pasta...** para abrir esse

diretório em uma nova janela do Windows explorer.

### 4.6.14 Licenças

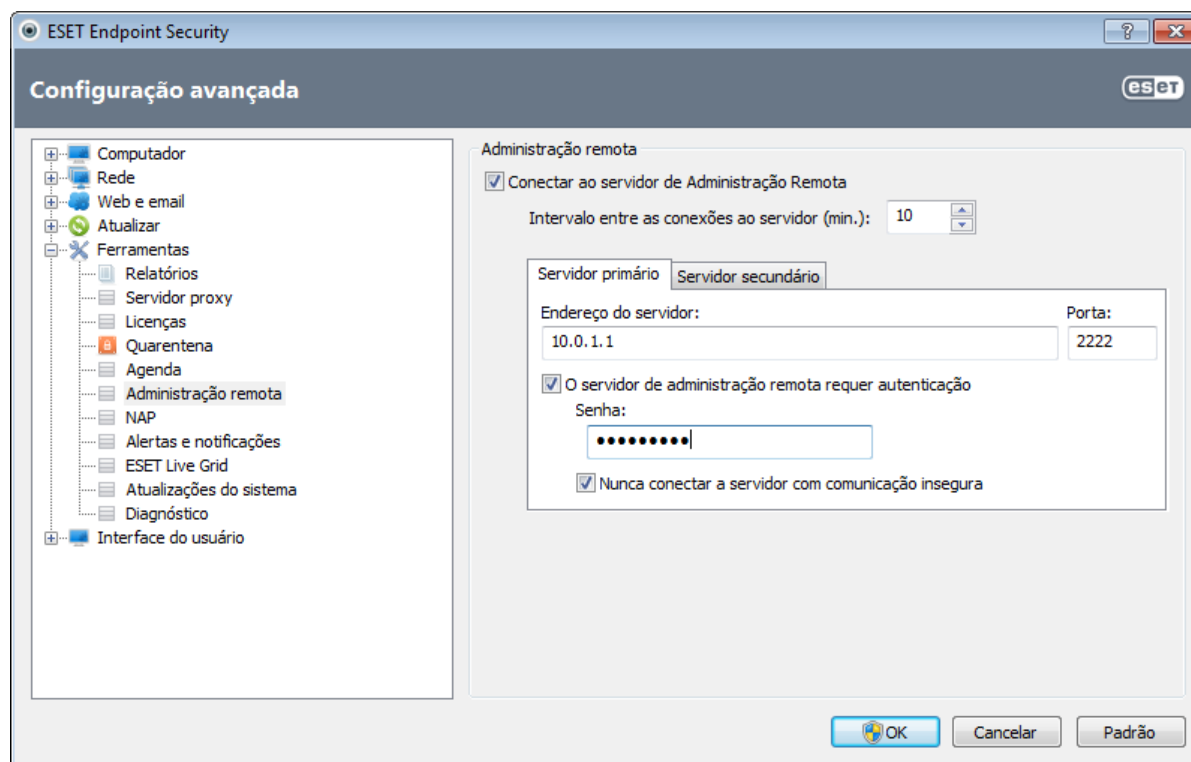
A ramificação **Licenças** permite gerenciar as chaves de licença do ESET Endpoint Security e de outros produtos da ESET, como o ESET Remote Administrator etc. Após a compra, as chaves de licença são fornecidas com o nome de usuário e a senha. Para **Adicionar/Remover** uma chave de licença, clique no botão correspondente na janela (**Licenças**) do gerenciador de licenças. O gerenciador de licenças pode ser acessado na árvore Configuração avançada clicando em **Ferramentas** > **Licenças**.

A chave de licença é um arquivo de texto que contém informações sobre o produto comprado: o proprietário, o número de licenças e a data de expiração.

A janela do gerenciador de licenças permite carregar e visualizar o conteúdo de uma chave de licença usando o botão **Adicionar...** - as informações contidas serão exibidas no gerenciador. Para excluir um arquivo de licença da lista, selecione-o e clique em **Remover**.

Se uma chave de licença tiver expirado e você estiver interessado em adquirir a renovação, clique no botão **Solicitar...**; você será redirecionado à nossa loja on-line.

### 4.6.15 Administração remota

O ESET Remote Administrator (ERA) é uma ferramenta poderosa para gerenciar a política de segurança e para obter uma visão geral de toda a segurança em uma rede. É especialmente útil quando aplicada a redes maiores. O ERA não aumenta somente o nível de segurança, mas também fornece facilidade de uso no gerenciamento do ESET Endpoint Security em estações de trabalho clientes. É possível instalar, configurar, exibir arquivos de log, agendar tarefas de atualização, rastrear tarefas etc. A comunicação entre o ESET Remote Administrator (ERAS) e os produtos de segurança da ESET requer uma configuração correta em ambos os pontos de extremidade.

As opções de configuração de administração remota estão disponíveis na janela principal do programa ESET Endpoint Security. Clique em **Configuração** > **Entrar na configuração avançada...** > **Ferramentas** > **Administração remota**.

Ative a administração remota selecionando a opção **Conectar ao servidor de Administração remota**. É possível acessar as outras opções descritas a seguir:

**Intervalo entre as conexões ao servidor (min.)** - É indicada a frequência com que o produto de segurança da ESET se conectará ao ERAS para enviar os dados.

**Servidor primário, Servidor secundário** - Geralmente, apenas o servidor primário precisa ser configurado. Se estiver executando diversos servidores ERA na rede, você pode optar por adicionar outra conexão do servidor secundário ERA. Servirá como a solução de fallback. Portanto, se o servidor primário tornar-se inacessível, a solução de segurança da ESET entrará em contato automaticamente com o servidor secundário ERA. Simultaneamente, ela tentará reestabelecer a conexão com o servidor primário. Após essa conexão estar ativa novamente, a solução de segurança da ESET retornará ao servidor primário. A configuração de dois servidores de administração remota é mais adequada para clientes móveis com notebooks que se conectam na rede local e fora da rede.

**Endereço do servidor** - Especifique o nome DNS ou endereço IP do servidor que está executando o ERAS.

**Porta** - Esse campo contém um valor predefinido utilizado para conexão. Recomendamos que você deixe a configuração de porta padrão em 2222.

**Intervalo entre as conexões ao servidor (min.)** - Essa opção designa a frequência com que o ESET Endpoint Security conectará ao ERA Server. Se estiver configurado como 0, as informações serão enviadas a cada 5 segundos.

**O servidor do Administrador remoto requer autenticação** - Permite inserir uma senha para conectar-se ao ERA Server, se solicitada.

**Nunca conectar a servidor com comunicação insegura** - Selecione essa opção para desativar a conexão com os servidores ERA onde o acesso não autenticado estiver ativado (consulte **ERA Console** > **Opções do servidor** > **Segurança** > **Permitir acesso não autenticado para clientes**).

Clique em **OK** para confirmar as alterações e aplicar as configurações. O ESET Endpoint Security as usará para conectar-

se ao servidor ERA Server.

## 4.7 Interface do usuário

A seção **Interface do usuário** permite configurar o comportamento da GUI (Graphical User Interface, interface gráfica do usuário) do programa.

Usando a ferramenta Gráficos, é possível ajustar a aparência visual do programa e os efeitos usados.

Ao configurar Alertas e notificações, você pode alterar o comportamento de alertas de ameaças detectadas e notificações do sistema. Esses recursos podem ser personalizados de acordo com suas necessidades.

Se você escolher não exibir algumas notificações, elas serão exibidas na área Janelas de notificação ocultas. Aqui é possível verificar o status dessas notificações, mostrar mais detalhes ou removê-las dessa janela.

Para obter a máxima segurança do seu software, você pode evitar quaisquer alterações não autorizadas protegendo as configurações com uma senha com a ajuda da ferramenta Configuração de acesso.

O Menu de contexto é exibido após um clique com o botão direito do mouse no objeto selecionado. Utilize essa ferramenta para integrar os elementos de controle do ESET Endpoint Security no menu de contexto.

O Modo de apresentação é útil para usuários que pretendem trabalhar com um aplicativo, sem serem interrompidos por janelas pop-up, tarefas agendadas ou quaisquer componentes que possam carregar o processador e a RAM.

### 4.7.1 Gráficos

As opções de configuração da interface do usuário no ESET Endpoint Security permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções de configuração são acessíveis na ramificação **Interface do usuário** > **Gráficos** da árvore Configuração avançada do ESET Endpoint Security.

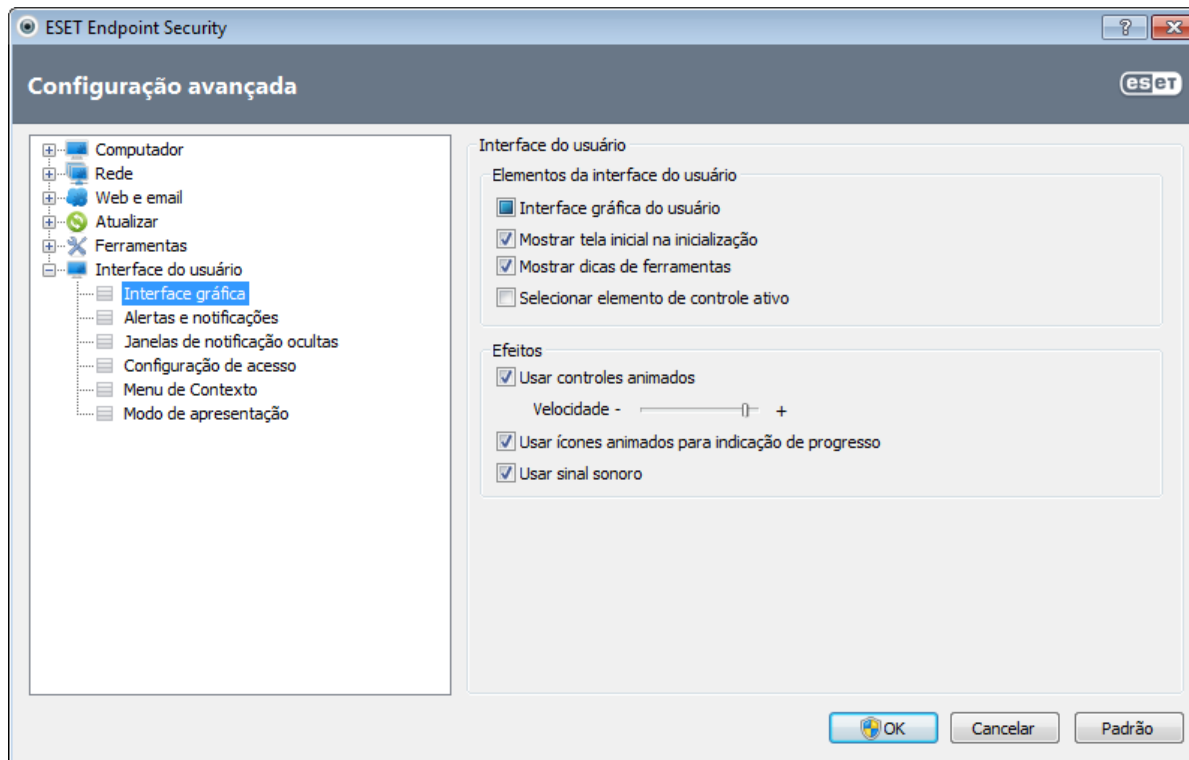
Na seção **Elementos da interface do usuário**, a opção **Interface gráfica do usuário** deve ser desativada se os elementos gráficos reduzirem o desempenho do seu computador ou provocarem outros problemas. A interface gráfica também pode precisar ser desativada para usuários com deficiência visual, uma vez que pode causar conflito com aplicativos especiais usados para leitura do texto exibido na tela.

Se desejar desativar a tela inicial do ESET Endpoint Security, desmarque a opção **Mostrar tela inicial na inicialização**.

Se a opção **Mostrar dicas de ferramentas** estiver ativada, uma descrição breve de qualquer opção será exibida quando o cursor for colocado em cima de uma opção. A opção **Selecionar elemento de controle ativo** fará com que o sistema destaque qualquer elemento que esteja atualmente na área ativa do cursor do mouse. O elemento realçado será ativado após um clique no mouse.

Para diminuir ou aumentar a velocidade dos efeitos animados, selecione a opção **Usar controles animados** e mova a barra deslizante **Velocidade** para a esquerda ou para a direita.

Para ativar o uso de ícones animados para exibir o andamento de várias operações, selecione a opção **Usar ícones animados para indicação de progresso**.

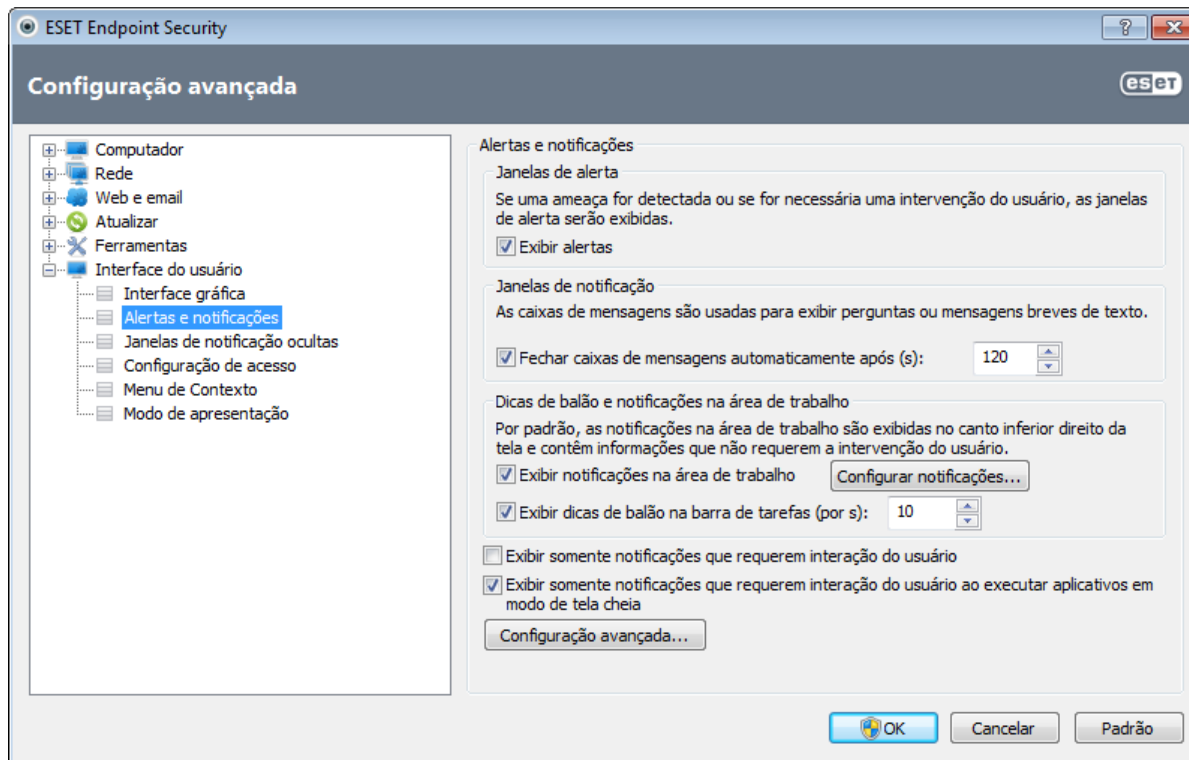
Se desejar que o programa emita um aviso sonoro se um evento importante ocorrer, selecione a opção **Usar sinal sonoro**. Observe que esse som será reproduzido somente quando um rastreamento de computador estiver em execução ou tiver sido concluído.

## 4.7.2 Alertas e notificações

A seção **Alertas e notificações** em **Interface do usuário** permite que você configure como os alertas de ameaças e as notificações do sistema (por exemplo, mensagens de atualização bem-sucedida) são tratados no ESET Endpoint Security. Você também pode definir a hora e o nível de transparência das notificações da bandeja do sistema (aplica-se somente aos sistemas compatíveis com notificações na bandeja do sistema).

O primeiro item é **Exibir alertas**. A desativação dessa opção cancelará todas as janelas de alerta e é adequada apenas para uma quantidade limitada de situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

Para fechar as janelas pop-up automaticamente após um certo período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente depois de (s)**. Se não forem fechadas manualmente, as janelas de alertas serão fechadas automaticamente após o período de tempo especificado expirar.

As notificações na área de trabalho e as dicas de balão são apenas informativas e não requerem nem proporcionam interação com o usuário. Elas são exibidas na área de notificação, no canto inferior direito da tela. Para ativar as notificações na área de trabalho, selecione a opção **Exibir notificações na área de trabalho**. Opções mais detalhadas, como o tempo de exibição e a transparência da janela de notificação, podem ser modificadas clicando no botão **Configurar notificações...** Para visualizar o comportamento das notificações, clique no botão **Visualizar**.

Para configurar a duração do tempo de exibição das dicas de balão, consulte a opção **Exibir dicas de balão na barra de tarefas (por s)** e insira o intervalo desejado no campo adjacente.

A opção **Exibir somente notificações que requerem interação do usuário** permite ativar/desativar alertas e notificações que não requeiram interação do usuário. Selecione **Exibir somente notificações que requerem interação do usuário ao executar aplicativos em modo de tela inteira** para suprimir todas as notificações que não sejam interativas.

Clique em **Configuração avançada...** para inserir opções de configuração adicionais de **Alertas e notificações**.

### 4.7.2.1 Configuração avançada

No menu suspenso **Detalhamento mínimo de eventos para exibir**, é possível selecionar o nível de gravidade inicial dos alertas e das notificações a serem exibidos.

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, a firewall pessoal, etc...).

O último recurso dessa seção permite configurar o destino das notificações em um ambiente com vários usuários. O campo **Em sistemas com vários usuários, exibir as notificações na tela deste usuário** especifica um usuário que receberá notificações do sistema e outras notificações sobre os sistemas, permitindo que diversos usuários se conectem ao mesmo tempo. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Esta opção é especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

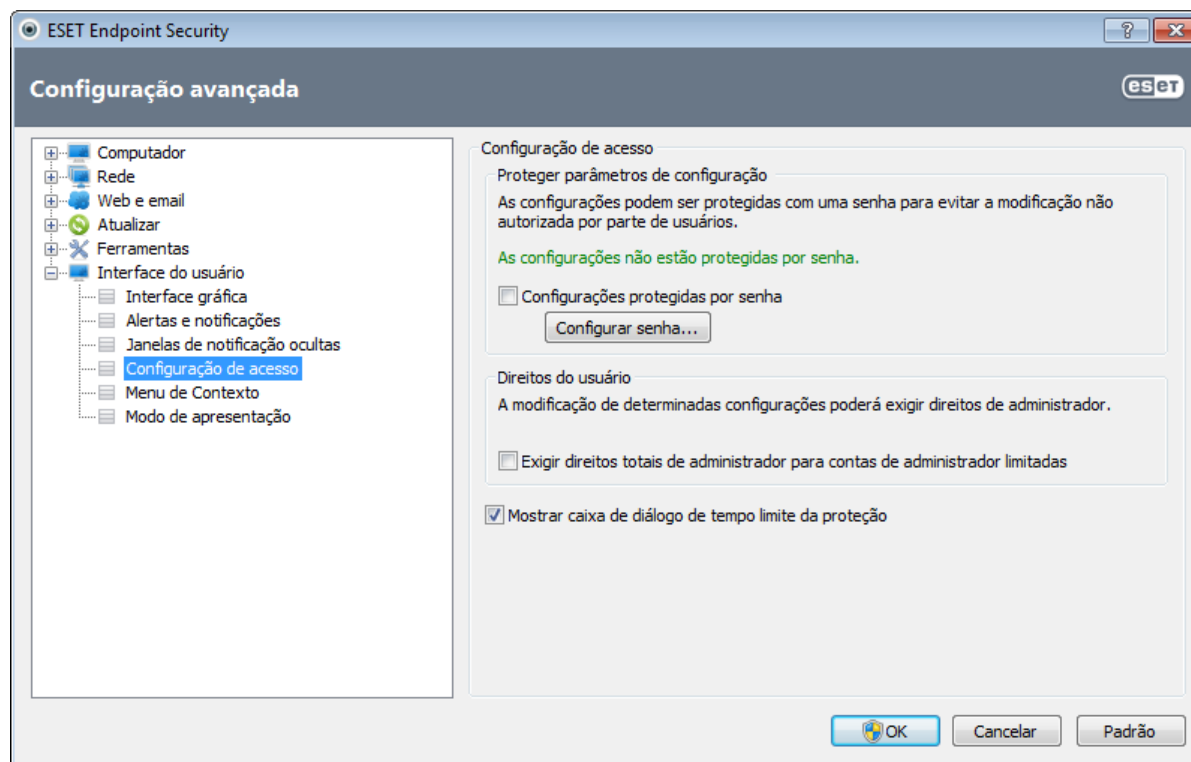
## 4.7.3 Janelas de notificação ocultas

Se a opção **Não exibir esta mensagem novamente** foi selecionada para qualquer janela de notificação (alerta) que foi exibida anteriormente, ela aparecerá na lista de janelas de notificações ocultas. As ações que agora são executadas automaticamente serão exibidas na coluna cujo título é **Confirmar**.

**Mostrar** - Mostra uma visualização das janelas de notificação que não são exibidas no momento e para as quais uma ação automática está configurada.

**Remover** - Remove itens da lista de **Caixas de mensagens ocultas**. Todas as janelas de notificação removidas da lista serão exibidas novamente.

### 4.7.4 Configuração do acesso

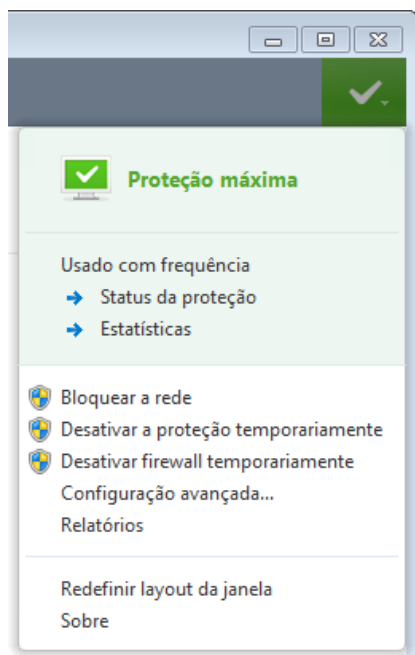
Para fornecer o máximo de segurança para o seu sistema, é essencial que o ESET Endpoint Security seja configurado corretamente. Qualquer alteração não qualificada pode resultar em perda de dados importantes. Essa opção está localizada no submenu **Configuração de acesso** em **Interface do usuário** na árvore Configuração avançada. Para evitar modificações não autorizadas, os parâmetros de configuração do ESET Endpoint Security podem ser protegidos por senha.

**Configurações protegidas por senha** - Bloqueia/desbloqueia os parâmetros de configuração do programa. Marque ou desmarque a caixa de seleção para abrir a janela de configuração Senha.

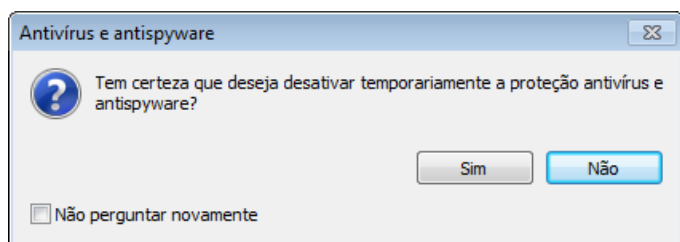
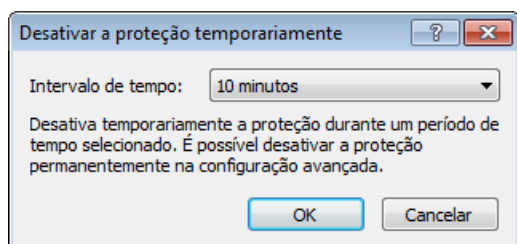
Para definir uma senha para proteger os parâmetros de configuração, clique em **Configurar senha...**

**Exigir direitos totais de administrador para contas de administrador limitadas** - Selecione essa opção para solicitar que o usuário atual (se ele não tiver direitos de administrador) digite o nome de usuário e a senha de administrador quando modificar determinados parâmetros do sistema (semelhante ao UAC no Windows Vista). As modificações incluem a desativação dos módulos de proteção ou a desativação do firewall.

**Mostrar caixa de diálogo de tempo limite da proteção** - Será solicitado a definir se essa opção for selecionada ao desativar temporariamente a proteção do menu do programa ou através da seção **ESET Endpoint Security** > **Configuração**. Um menu suspenso **Intervalo de tempo** na janela **Desativar a proteção temporariamente** representa o período de tempo durante o qual todos os componentes de proteção selecionados permanecerão desativados.

### 4.7.5 Menu do programa

No menu principal do programa estão disponíveis alguns dos recursos e opções de configuração mais importantes.

**Usado com frequência** - Exibe as extensões mais utilizadas do ESET Endpoint Security. Você pode acessar rapidamente esses objetos a partir do menu do programa.

**Desativar a proteção temporariamente** - Exibe a caixa de diálogo de confirmação que desativa a Proteção antivírus e antispyware, que protege contra ataques maliciosos ao sistema controlando arquivos e a comunicação via web e por emails. Marque a caixa de seleção **Não perguntar novamente** para evitar que essa mensagem seja exibida no futuro.

O menu suspenso **Intervalo de tempo** representa o período de tempo em que a proteção antivírus e antispyware será desativada.

**Bloquear o tráfego de rede** - O firewall pessoal bloqueará todo o tráfego de entrada e saída da rede e da Internet.

**Desativar firewall temporariamente** - Alterna o firewall para o estado inativo. Consulte o capítulo Integração do sistema do firewall pessoal para obter mais informações.

**Configuração avançada...** - Selecione essa opção para acessar a árvore **Configuração avançada**. Existem também outras formas de abri-lo, como, por exemplo, pressionando a tecla F5 ou navegando até **Configuração** > **Entrar na configuração avançada...**.

**Arquivos de log** - Os arquivos de log contêm informações sobre todos os eventos importantes do programa que ocorreram e fornece uma visão geral das ameaças detectadas.

**Redefinir layout da janela** - Redefine a janela do ESET Endpoint Security para seu tamanho e posição padrão na tela.

**Sobre** - As informações do sistema fornecem detalhes sobre a versão instalada do ESET Endpoint Security e os

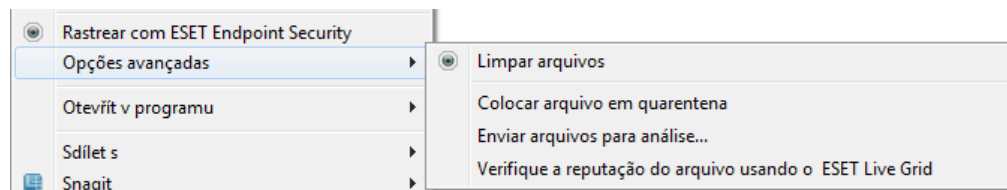
componentes do programa instalados. Você pode encontrar também aqui a data de expiração da licença. Na parte inferior, você encontra as informações sobre o sistema operacional e os recursos do sistema.

### 4.7.6 Menu de contexto

O menu de contexto é exibido após um clique com o botão direito do mouse no objeto selecionado. O menu lista todas as opções disponíveis para executar no objeto.

É possível integrar os elementos de controle do ESET Endpoint Security no menu de contexto. Opções de configuração mais detalhadas para essa funcionalidade estão disponíveis na árvore Configuração avançada em **Interface do usuário** > **Menu de contexto**.

**Integrar ao menu de contexto** - Integra os elementos de controle do ESET Endpoint Security no menu de contexto.

Rastrear com ESET Endpoint Security
Opções avançadas
Otevřít v programu
Sdílet s
Snagit
Limpar arquivos
Colocar arquivo em quarentena
Enviar arquivos para análise...
Verifique a reputação do arquivo usando o ESET Live Grid

As seguintes opções estão disponíveis no menu suspenso **Tipo de menu**:

- **Completo (rastrear primeiro)** - Ativa todas as opções do menu de contexto; o menu principal exibirá a opção **Rastrear com ESET Endpoint Security**.
- **Completo (limpar primeiro)** - Ativa todas as opções do menu de contexto; o menu principal exibirá a opção **Limpar com ESET Endpoint Security**.
- **Apenas rastrear** - Somente a opção **Rastrear com ESET Endpoint Security** será exibida no menu de contexto.
- **Apenas limpar** - Somente a opção **Limpar com ESET Endpoint Security** será exibida no menu de contexto.

### 4.7.7 Modo de apresentação

Modo de apresentação é um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Modo de apresentação também pode ser utilizado durante apresentações que não podem ser interrompidas pela atividade do antivirus. Ao ativar esse recurso, todas as janelas pop-up são desativadas e a atividade da agenda será completamente interrompida. A proteção do sistema ainda é executada em segundo plano, mas não requer interação com nenhum usuário.

É possível ativar ou desativar o Modo de apresentação na janela principal do programa clicando em **Configuração** > **Computador** e, em seguida, em **Ativar** em **Modo de apresentação** na árvore Configuração avançada (F5) ao expandir **Interface do usuário**, clicar em **Modo de apresentação** e marcar a caixa de seleção próxima a **Ativar Modo de apresentação**. Ativar o Modo de apresentação é um risco de segurança em potencial, pois o ícone do status de proteção na barra de tarefas ficará laranja e exibirá um aviso. Também será possível ver este aviso na janela do programa principal onde verá Modo de apresentação ativado em laranja.

Ao selecionar a caixa de seleção **Ativar automaticamente o Modo de apresentação ao executar aplicativos em tela cheia**, o Modo de apresentação será iniciado depois que você iniciar um aplicativo em tela cheia e será interrompido automaticamente ao sair do aplicativo. Esse recurso é especialmente útil para iniciar o Modo de apresentação logo após iniciar um jogo, abrir um aplicativo em tela cheia ou iniciar uma apresentação.

Também é possível marcar **Desativar o Modo de apresentação automaticamente após X minutos** na caixa de seleção para definir o período de tempo (o valor padrão é 1 minuto). Essa função será útil quando você quer usar o Modo de apresentação apenas por um determinado período de tempo e pretende desativá-lo logo depois.

**OBSERVAÇÃO:** Se o firewall pessoal estiver no modo interativo e o Modo de apresentação for ativado, você pode ter dificuldades para conectar-se à Internet. Isso pode ser um problema se você iniciar um jogo on-line. Normalmente, você será solicitado a confirmar tal ação (se não houver regras de comunicação ou exceções definidas), mas a interação com o usuário é desativada no Modo de apresentação. A solução é definir uma regra de comunicação para cada aplicativo que possa estar em conflito com esse comportamento ou usar outro Modo de filtragem no firewall pessoal. Tenha em mente também que, se o Modo de apresentação estiver ativado e você acessar uma página da web ou um aplicativo que possa ser considerado um risco à segurança, eles poderão ser bloqueados e nenhuma explicação ou aviso serão exibidos devido à desativação da interação com o usuário.

# 5. Usuário avançado

## 5.1 Configuração do servidor proxy

Em grandes redes, a conexão do seu computador com a Internet pode ser mediada por um servidor proxy. Se esse for o caso, as configurações a seguir precisarão ser definidas. Caso contrário, o programa não poderá se atualizar automaticamente. No ESET Endpoint Security, a configuração do servidor proxy está disponível em duas seções diferentes na árvore Configuração avançada.

As configurações do servidor proxy podem ser definidas em **Configuração avançada**, em **Ferramentas** > **Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET Endpoint Security. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

Para especificar as configurações do servidor proxy para esse nível, marque a caixa de seleção **Usar servidor proxy** e digite o endereço do servidor proxy no campo **Servidor proxy**, junto com o número da **Porta** do servidor proxy.

Se a comunicação com o servidor proxy exigir autenticação, marque a caixa de seleção **O servidor proxy requer autenticação** e digite um **Usuário** e uma **Senha** válidos nos respectivos campos. Clique no botão **Detectar servidor proxy** para detectar e preencher automaticamente as configurações do servidor proxy. Os parâmetros especificados no Internet Explorer serão copiados.

**OBSERVAÇÃO:** Esse recurso não recupera dados de autenticação (nome de usuário e senha); eles devem ser fornecidos por você.

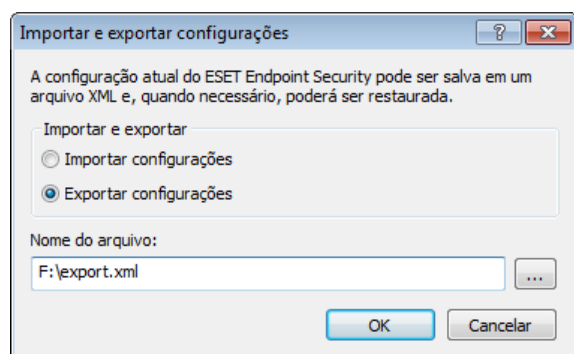
As configurações do servidor proxy também podem ser estabelecidas na Configuração avançada de atualização (ramificação **Atualizar** da árvore **Configuração avançada**). Essa configuração será aplicada ao perfil de atualização especificado e é recomendada para laptops que recebem frequentemente atualizações de assinatura de vírus de diferentes locais. Para obter mais informações sobre essa configuração, consulte a seção Configuração avançada de atualização.

## 5.2 Importar e exportar configurações

A importação e a exportação das configurações do ESET Endpoint Security estão disponíveis em **Configuração**.

Tanto a importação quanto a exportação usam o tipo de arquivo .xml. A importação e a exportação serão úteis caso precise fazer backup da configuração atual do ESET Endpoint Security para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários que desejam utilizar as suas configurações preferenciais do ESET Endpoint Security em diversos sistemas. Os usuários podem importar facilmente um arquivo .xml para transferir as configurações desejadas.

A importação de uma configuração é muito fácil. Na janela principal do programa, clique em **Configuração** > **Importar e exportar configurações...** e selecione a opção **Importar configurações**. Digite o caminho para o arquivo de configuração ou clique no botão **...** para procurar o arquivo de configuração que deseja importar.

As etapas para exportar uma configuração são muito semelhantes. Na janela principal do programa, clique em **Configuração** > **Importar e exportar configurações...**. Selecione a opção **Exportar configurações** e insira o **Nome de arquivo** do arquivo de configuração (ou seja, export.xml). Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.

## 5.3 Atalhos do teclado

As teclas de atalho que podem ser usadas ao trabalhar com o ESET Endpoint Security incluem:

| | |
|---|---|
| Ctrl+G | desativa a GUI no produto |
| Ctrl+I | abre a página do ESET SysInspector |
| Ctrl+L | abre a página Arquivos de log |
| Ctrl+S | abre a página Agenda |
| Ctrl+Q | abre a página Quarentena |
| Ctrl+U | abre a janela da caixa de diálogo onde o Nome de usuário e a Senha podem ser definidos |
| Ctrl+R | redefine a janela para seu tamanho e posição padrão na tela. |

Para uma melhor navegação no produto de segurança ESET, os seguintes atalhos de teclado podem ser utilizados:

| | |
|---|---|
| F1 | abre as páginas da Ajuda |
| F5 | abre a Configuração avançada |
| Up/Down | permite a navegação no produto por itens |
| * | expande o nó da árvore de Configuração avançada |
| - | recolhe o nó da árvore de Configuração avançada |
| TAB | move o cursor em uma janela |
| Esc | fecha a janela da caixa de diálogo ativa |

## 5.4 Linha de comando

O módulo antivírus do ESET Endpoint Security pode ser iniciado pela linha de comando – manualmente (com o comando "ecls") ou com um arquivo em lotes ("bat"). Uso para o rastreamento por linha de comando da ESET:

```
ecls [OPTIONS..] FILES..
```

Os seguintes parâmetros e chaves podem ser utilizados ao executar o scanner sob demanda na linha de comando:

**Opções**

| | |
|---|---|
| /base-dir=PASTA | carregar módulos da PASTA |
| /quar-dir=PASTA | PASTA de quarentena |
| /exclude=MÁSCARA | excluir arquivos que correspondem à MÁSCARA do rastreamento |
| /subdir | rastrear subpastas (padrão) |
| /no-subdir | não rastrear subpastas |
| /max-subdir-level=NÍVEL | subnível máximo de pastas dentro de pastas para rastrear |
| /symlink | seguir links simbólicos (padrão) |
| /no-symlink | ignorar links simbólicos |
| /ads | rastrear ADS (padrão) |
| /no-ads | não rastrear ADS |
| /log-file=ARQUIVO | registrar o relatório em ARQUIVO |
| /log-rewrite | substituir arquivo de saída (padrão - acrescentar) |
| /log-console | registrar saída para console (padrão) |
| /no-log-console | não registrar saída para console |
| /log-all | também registrar arquivos limpos |
| /no-log-all | não registrar arquivos limpos (padrão) |
| /aind | mostrar indicador de atividade |
| /auto | rastrear e limpar automaticamente todos os discos locais |

**Opções do scanner**

| | |
|---|---|
| /files | rastrear arquivos (padrão) |
| /no-files | não rastrear arquivos |
| /memory | rastrear memória |
| /boots | rastrear setores de inicialização |
| /no-boots | não rastrear setores de inicialização (padrão) |
| /arch | rastrear arquivos compactados (padrão) |
| /no-arch | não rastrear arquivos compactados |
| /max-obj-size=TAMANHO | rastrear apenas arquivos com menos de TAMANHO megabytes (padrão 0 = sem limite) |
| /max-arch-level=NÍVEL | subnível máximo de arquivos dentro de arquivos (arquivos aninhados) para rastrear |
| /scan-timeout=LIMITE | rastrear arquivos pelo LIMITE máximo de segundos |

| | |
|---|---|
| /max-arch-size=TAMANHO | rastrear apenas os arquivos em um arquivo compactado se eles tiverem menos de TAMANHO (padrão 0 = sem limite) |
| /max-sfx-size=TAMANHO | rastrear apenas os arquivos em um arquivo compactado de auto-extração se eles tiverem menos de TAMANHO megabytes (padrão 0 = sem limite) |
| /mail | rastrear arquivos de email (padrão) |
| /no-mail | não rastrear arquivos de email |
| /mailbox | rastrear caixas de correio (padrão) |
| /no-mailbox | não rastrear caixas de correio |
| /sfx | rastrear arquivos compactados de auto-extração (padrão) |
| /no-sfx | não rastrear arquivos compactados de auto-extração |
| /rtp | rastrear empacotadores em tempo real (padrão) |
| /no-rtp | não rastrear empacotadores em tempo real |
| /adware | rastrear se há Adware/Spyware/Riskware (padrão) |
| /no-adware | não rastrear se há Adware/Spyware/Riskware |
| /unsafe | rastrear por aplicativos potencialmente inseguros |
| /no-unsafe | não rastrear por aplicativos potencialmente inseguros (padrão) |
| /unwanted | rastrear por aplicativos potencialmente indesejados |
| /no-unwanted | não rastrear por aplicativos potencialmente indesejados (padrão) |
| /pattern | usar assinaturas (padrão) |
| /no-pattern | não usar assinaturas |
| /heur | ativar heurística (padrão) |
| /no-heur | desativar heurística |
| /adv-heur | ativar heurística avançada (padrão) |
| /no-adv-heur | desativar heurística avançada |
| /ext=EXTENSÕES | verificar somente EXTENSÕES delimitadas por dois pontos |
| /ext-exclude=EXTENSÕES | excluir do rastreamento EXTENSÕES delimitadas por dois pontos |
| /clean-mode=MODO | utilizar MODO de limpeza para objetos infectados.<br>Opções disponíveis: none (nenhum), standard (padrão), strict (rígida), rigorous (rigorosa), delete (excluir) |
| /quarantine | copiar arquivos infectados para Quarentena<br>(completa a ação realizada enquanto ocorre a limpeza) |
| /no-quarantine | não copiar arquivos infectados para Quarentena |

**Opções gerais**

| | |
|---|---|
| /help | mostrar ajuda e sair |
| /version | mostrar informações de versão e sair |
| /preserve-time | manter último registro de acesso |

**Códigos de saída**

| | |
|---|---|
| 0 | nenhuma ameaça encontrada |
| 1 | ameaça encontrada e removida |
| 10 | alguns arquivos não puderam ser rastreados (podem conter ameaças) |
| 50 | ameaça encontrada |
| 100 | erro |

**OBSERVAÇÃO:** Os códigos de saída maiores que 100 significam que o arquivo não foi rastreado e, portanto, pode estar infectado.

## 5.5 ESET SysInspector

### 5.5.1 Introdução ao ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o seu computador e exibe os dados coletados de uma maneira abrangente. Informações como drivers e aplicativos instalados, conexões de rede ou entradas importantes de registro podem ajudá-lo a investigar o comportamento suspeito do sistema, seja devido a incompatibilidade de software ou hardware ou infecção por malware.

É possível acessar o ESET SysInspector de duas formas: Na versão integrada nas soluções ESET Security ou por meio de download da versão autônoma (SysInspector.exe) gratuita no site da ESET. Ambas as versões têm funções idênticas e os mesmos controles de programa. A única diferença é a forma como os resultados são gerenciados. As versões autônoma e integrada permitem exportar instantâneos do sistema em um arquivo .xml e salvá-los em disco. Entretanto, a versão integrada também permite armazenar os instantâneos do sistema diretamente em **Ferramentas** > **ESET SysInspector** (exceto ESET Remote Administrator).

Aguarde enquanto o ESET SysInspector rastreia o computador. Pode demorar de 10 segundos a alguns minutos,

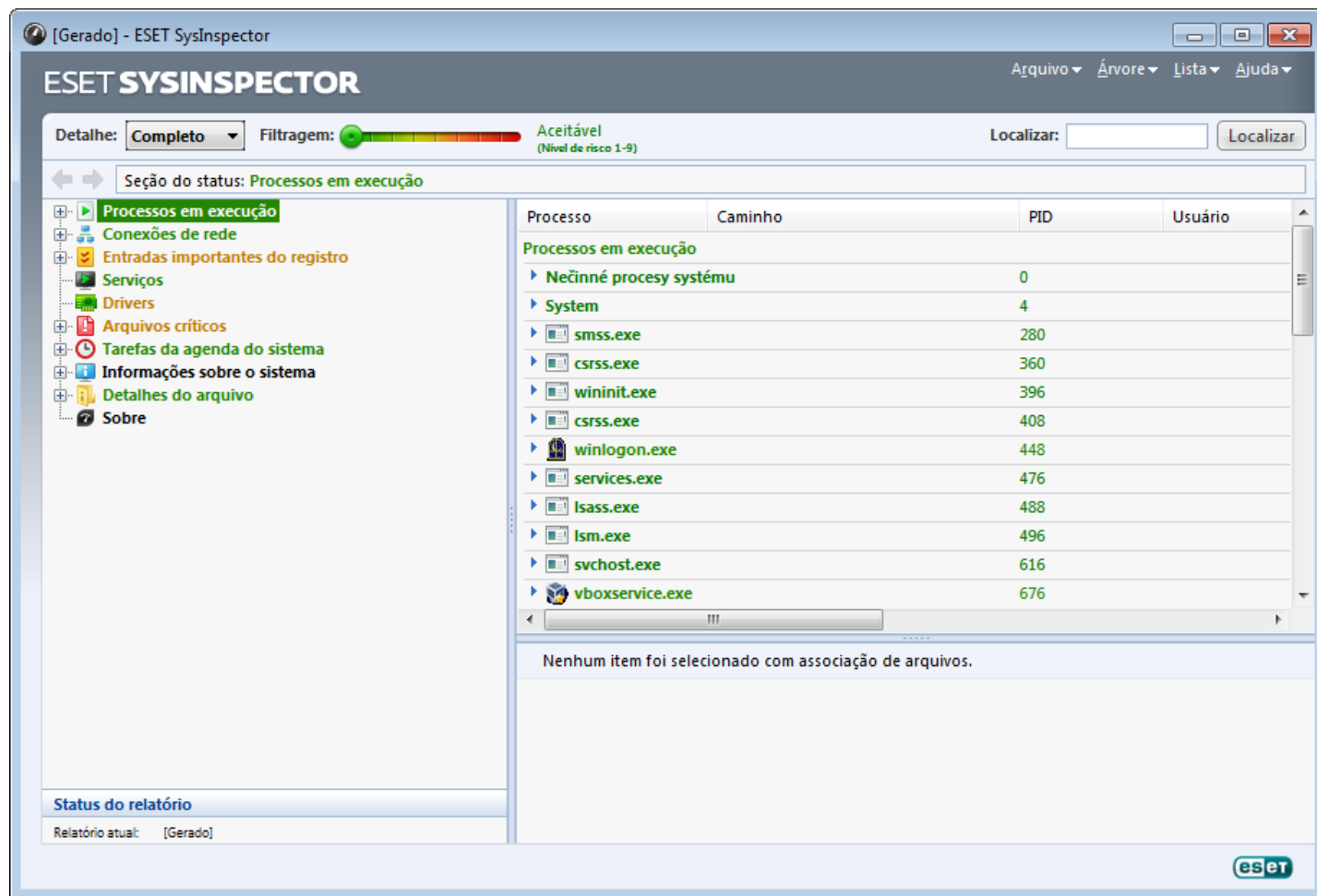
dependendo da configuração de hardware, do sistema operacional e da quantidade de aplicativos instalados no computador.

#### 5.5.1.1 Inicialização do ESET SysInspector

Para iniciar o ESET SysInspector, basta executar o arquivo executável SysInspector.exe obtido por download no site da ESET.

Aguarde enquanto o aplicativo inspeciona o sistema, o que pode demorar vários minutos, dependendo do hardware e dos dados a serem coletados.

### 5.5.2 Interface do usuário e uso do aplicativo

Para maior clareza, a janela principal é dividida em quatro seções principais - Controles do programa localizados na parte superior da janela principal, a janela Navegação à esquerda, a janela Descrição à direita, no meio, e a janela Detalhes à direita, na parte inferior da janela principal. A seção Status do log lista os parâmetros básicos de um log (filtro usado, tipo de filtro, se o log é o resultado de uma comparação, etc.).

#### 5.5.2.1 Controles do programa

Esta seção contém a descrição de todos os controles do programa disponíveis no ESET SysInspector.

**Arquivo**

Clicando em **Arquivo**, você pode armazenar o status atual do sistema para investigação posterior ou abrir um log armazenado anteriormente. Por motivo de publicação, recomendamos a geração de um log **Adequado para envio**. Neste formulário, o log omite informações confidenciais (nome do usuário atual, nome do computador, nome do domínio, privilégios do usuário atual, variáveis do ambiente, etc.).

**OBSERVAÇÃO:** Você pode abrir os relatórios do ESET SysInspector armazenados anteriormente simplesmente arrastando e soltando-os na janela principal.

**Árvore**

Permite expandir ou fechar todos os nós e exportar as seções selecionadas para o script de serviços.

**Lista**

Contém funções para uma navegação mais fácil dentro do programa e diversas outras funções, como, por exemplo, encontrar informações online.

**Ajuda**

Contém informações sobre o aplicativo e as funções dele.

**Detalhe**

Esta configuração influencia as informações exibidas na janela principal para facilitar o trabalho com as informações. No modo "Básico", você terá acesso a informações utilizadas para encontrar soluções para problemas comuns no seu sistema. No modo "Médio", o programa exibe detalhes menos usados. No modo "Completo", o ESET SysInspector exibe todas as informações necessárias para resolver problemas muito específicos.

**Filtragem de itens**

A filtragem de itens é mais adequada para encontrar arquivos suspeitos ou entradas do registro no sistema. Ajustando o controle deslizante, você pode filtrar itens pelo nível de risco deles. Se o controle deslizante estiver configurado todo para a esquerda (Nível de risco 1), todos os itens serão exibidos. Se você mover o controle deslizante para a direita, o programa filtrará todos os itens menos perigosos que o nível de risco atual e exibirá apenas os itens que são mais suspeitos que o nível exibido. Com o controle deslizante todo para a direita, o programa exibirá apenas os itens perigosos conhecidos.

Todos os itens identificados como de risco 6 a 9 podem colocar a segurança em risco. Se você não estiver utilizando uma solução de segurança da ESET, recomendamos que você rastreie o sistema com o ESET Online Scanner se o ESET SysInspector encontrou esse item. O ESET Online Scanner é um serviço gratuito.

**OBSERVAÇÃO:** O nível de risco de um item pode ser rapidamente determinado comparando a cor do item com a cor no controle deslizante Nível de risco.

**Pesquisar**

A opção Pesquisar pode ser utilizada para encontrar um item específico pelo nome ou por parte do nome. Os resultados da solicitação da pesquisa são exibidos na janela Descrição.

**Retornar**

Clicando na seta para trás e para a frente, você pode retornar para as informações exibidas anteriormente na janela Descrição. Você pode usar as teclas Backspace e de espaço em vez de clicar para trás e para a frente.

**Seção do status**

Exibe o nó atual na janela Navegação.

**Importante:** Os itens realçados em vermelho são desconhecidos, por isso o programa os marca como potencialmente perigosos. Se um item estiver em vermelho, isso não significa automaticamente que você pode excluir o arquivo. Antes de excluir, certifique-se de que os arquivos são realmente perigosos ou desnecessários.

### 5.5.2.2 Navegação no ESET SysInspector

O ESET SysInspector divide vários tipos de informações em diversas seções básicas chamadas de nós. Se disponíveis, você pode encontrar detalhes adicionais expandindo cada nó em seus subnós. Para abrir ou recolher um nó, clique duas vezes no nome do nó ou, como alternativa, clique em ⊞ ou em ⊟ próximo ao nome do nó. À medida que percorrer a estrutura em árvore dos nós e subnós na janela Navegação, você pode encontrar diversos detalhes para cada nó mostrado na janela Descrição. Se você percorrer os itens na janela Descrição, detalhes adicionais sobre cada item podem ser exibidos na janela Detalhes.

A seguir estão as descrições dos nós principais na janela Navegação e as informações relacionadas nas janelas Descrição e Detalhes.

**Processos em execução**

Esse nó contém informações sobre aplicativos e processos em execução no momento da geração do log. Na janela Descrição, você pode encontrar detalhes adicionais para cada processo, como, por exemplo, bibliotecas dinâmicas

usadas pelo processo e o local delas no sistema, o nome do fornecedor do aplicativo, o nível de risco do arquivo, etc.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

**OBSERVAÇÃO:** Um sistema operacional consiste em diversos componentes kernel importantes que são executados 24 horas por dia, 7 dias por semana e que fornecem funções básicas e vitais para outros aplicativos de usuários. Em determinados casos, tais processos são exibidos na ferramenta ESET SysInspector com o caminho do arquivo começando com \??\. Esses símbolos fornecem otimização de pré-início para esses processos; eles são seguros para o sistema.

**Conexões de rede**

A janela Descrição contém uma lista de processos e aplicativos que se comunicam pela rede utilizando o protocolo selecionado na janela Navegação (TCP ou UDP), junto com os endereços remotos aos quais o aplicativo está conectado. Também é possível verificar os endereços IP dos servidores DNS.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

**Entradas importantes do registro**

Contém uma lista de entradas de registro selecionadas que estão relacionadas freqüentemente a diversos problemas com o sistema, como aqueles que especificam os programas de inicialização, objetos auxiliares do navegador (BHO), etc.

Na janela Descrição, é possível localizar quais arquivos estão relacionados a entradas de registro específicas. Você pode consultar detalhes adicionais na janela Detalhes.

**Serviços**

A janela Descrição contém uma lista de arquivos registrados como serviços do Windows. É possível verificar a maneira como o serviço é configurado para iniciar, junto com detalhes específicos do arquivo na janela Detalhes.

**Drivers**

Uma lista de drivers instalados no sistema.

**Arquivos críticos**

A janela Descrição exibe o conteúdo dos arquivos críticos relacionados ao sistema operacional Microsoft Windows.

**Tarefas da agenda do sistema**

Contém uma lista de tarefas acionadas pela Agenda de Tarefas do Windows em uma hora/intervalo específico.

**Informações do sistema**

Contém informações detalhadas sobre hardware e software, além de informações sobre as variáveis ambientais configuradas, os direitos do usuário e os registros de eventos do sistema.

**Detalhes do arquivo**

Uma lista de arquivos importantes do sistema e arquivos na pasta Arquivos de programas. Informações adicionais específicas dos arquivos podem ser encontradas nas janelas Descrição e Detalhes.

**Sobre**

Informações sobre a versão do ESET SysInspector e a lista dos módulos do programa.

#### 5.5.2.2.1 Atalhos do teclado

As teclas de atalho que podem ser usadas ao trabalhar com o ESET SysInspector incluem:

**Arquivo**

| | |
|---|---|
| Ctrl+O | Abre o log existente |
| Ctrl+S | Salva os logs criados |

**Gerar**

| | |
|---|---|
| Ctrl+G | gera um instantâneo padrão do status do computador |
| Ctrl+H | gera um instantâneo do status do computador que também pode registrar informações confidenciais |

**Filtragem de itens**

| | |
|---|---|
| 1, O | Aceitável, nível de risco 1-9, os itens são exibidos |
| 2 | Aceitável, nível de risco 2-9, os itens são exibidos |
| 3 | Aceitável, nível de risco 3-9, os itens são exibidos |
| 4, U | Desconhecido, nível de risco 4-9, os itens são exibidos |
| 5 | Desconhecido, nível de risco 5-9, os itens são exibidos |
| 6 | Desconhecido, nível de risco 6-9, os itens são exibidos |
| 7, B | Perigoso, nível de risco 7-9, os itens são exibidos |
| 8 | Perigoso, nível de risco 8-9, os itens são exibidos |
| 9 | Perigoso, nível de risco 9, os itens são exibidos |
| - | Diminui o nível de risco |
| + | Aumenta o nível de risco |
| Ctrl+9 | Modo de filtragem, nível igual ou superior |
| Ctrl+O | Modo de filtragem, somente nível igual |

**Exibir**

| | |
|---|---|
| Ctrl+5 | Exibição por fornecedor, todos os fornecedores |
| Ctrl+6 | Exibição por fornecedor, somente Microsoft |
| Ctrl+7 | Exibição por fornecedor, todos os outros fornecedores |
| Ctrl+3 | Exibe detalhes completos |
| Ctrl+2 | Exibe detalhes da mídia |
| Ctrl+1 | Exibição básica |
| Backspace | Move um passo para trás |
| Espaço | Move um passo para a frente |
| Ctrl+W | Expande a árvore |
| Ctrl+Q | Recolhe a árvore |

**Outros controles**

| | |
|---|---|
| Ctrl+T | Vai para o local original do item após a seleção nos resultados de pesquisa |
| Ctrl+P | Exibe informações básicas sobre um item |
| Ctrl+A | Exibe informações completas sobre um item |
| Ctrl+C | Copia a árvore do item atual |
| Ctrl+X | Copia itens |
| Ctrl+B | Localiza informações sobre os arquivos selecionados na Internet |
| Ctrl+L | Abre a pasta em que o arquivo selecionado está localizado |
| Ctrl+R | Abre a entrada correspondente no editor do registro |
| Ctrl+Z | Copia um caminho para um arquivo (se o item estiver relacionado a um arquivo) |
| Ctrl+F | Alterna para o campo de pesquisa |
| Ctrl+D | Fecha os resultados da pesquisa |
| Ctrl+E | Executa script de serviços |

**Comparação**

| | |
|---|---|
| Ctrl+Alt+O | Abre o log original/comparativo |
| Ctrl+Alt+R | Cancela a comparação |
| Ctrl+Alt+1 | Exibe todos os itens |
| Ctrl+Alt+2 | Exibe apenas os itens adicionados; o log mostrará os itens presentes no log atual |
| Ctrl+Alt+3 | Exibe apenas os itens removidos; o log mostrará os itens presentes no log anterior |
| Ctrl+Alt+4 | Exibe apenas os itens substituídos (arquivos inclusive) |
| Ctrl+Alt+5 | Exibe apenas as diferenças entre os logs |

| | |
|---|---|
| Ctrl+Alt+C | Exibe a comparação |
| Ctrl+Alt+N | Exibe o log atual |
| Ctrl+Alt+P | Exibe o log anterior |

**Diversos**

| | |
|---|---|
| F1 | Exibe a Ajuda |
| Alt+F4 | Fecha o programa |
| Alt+Shift+F4 | Fecha o programa sem perguntar |
| Ctrl+I | Estatísticas de logs |

### 5.5.2.3 Comparar

O recurso Comparar permite que o usuário compare dois logs existentes. O resultado desse recurso é um conjunto de itens não comuns em ambos os logs. Ele é adequado se você desejar manter controle das alterações no sistema, uma ferramenta útil para detectar atividade de código malicioso.

Após ser iniciado, o aplicativo criará um novo log, que será exibido em uma nova janela. Navegue até **Arquivo** > **Salvar relatório** para salvar um log em um arquivo. Os arquivos de log podem ser abertos e visualizados posteriormente. Para abrir um log existente, utilize **Arquivo** > **Abrir relatório**. Na janela principal do programa, o ESET SysInspector sempre exibe um log de cada vez.

O benefício de comparar dois logs é que você pode visualizar um log ativo atual e um log salvo em um arquivo. Para comparar logs, utilize a opção **Arquivo** > **Comparar relatório** e escolha **Selecionar arquivo**. O log selecionado será comparado com o log ativo na janela principal do programa. O log comparativo exibirá somente as diferenças entre esses dois logs.

**OBSERVAÇÃO:** Caso compare dois arquivos de log, selecione **Arquivo** > **Salvar relatório** para salvá-lo como um arquivo ZIP; ambos os arquivos serão salvos. Se você abrir esse arquivo posteriormente, os logs contidos serão comparados automaticamente.

Próximo aos itens exibidos, o ESET SysInspector mostra símbolos que identificam diferenças entre os logs comparados.

Os itens marcados por um - apenas podem ser encontrados no log ativo e não estavam presentes no log comparativo aberto. Os itens marcados por um + estavam presentes apenas no log aberto e estavam ausentes no log ativo.

Descrição de todos os símbolos que podem ser exibidos próximos aos itens:

- + novo valor, não presente no log anterior
- a seção de estrutura em árvore contém novos valores
- - valor removido, presente apenas no log anterior
- a seção de estrutura em árvore contém valores removidos
- o valor/arquivo foi alterado
- a seção de estrutura em árvore contém valores/arquivos modificados
- o nível de risco reduziu / era maior no log anterior
- o nível de risco aumentou / era menor no log anterior

A seção de explicação exibida no canto inferior esquerdo descreve todos os símbolos e também exibe os nomes dos logs que estão sendo comparados.

**Status do relatório**

Relatório atual: SysInspector-ADMIN-PC-110728-1128.xml [Carregado-ZIP]
Relatório anterior: SysInspector-ADMIN-PC-110728-1132.xml [Carregado-ZIP]
Comparar: [Resultado da comparação]

**Comparar legendas de ícones**

| | |
|---|---|
| + Item adicionado | Item(ns) adicionado(s) em ramificação |
| − Item removido | Item(ns) removido(s) em ramificação |
| Arquivo substituído | Adicionado ou removido Item(ns) adicionado(s) em ramificação |
| Status foi rebaixado | |
| Status foi elevado | Arquivo(s) substituído(s) em ramificaçã |

Qualquer log comparativo pode ser salvo em um arquivo e aberto posteriormente.

**Exemplo**

Gere e salve um relatório, registrando informações originais sobre o sistema, em um arquivo chamado previous.xml. Após terem sido feitas as alterações, abra o ESET SysInspector e deixe-o gerar um novo relatório. Salve-o em um arquivo chamado current.xml.

Para controlar as alterações entre esses dois logs, navegue até **Arquivo** > **Comparar relatórios**. O programa criará um log comparativo mostrando as diferenças entre os logs.

O mesmo resultado poderá ser alcançado se você utilizar a seguinte opção da linha de comandos:

SysIsnpector.exe current.xml previous.xml

### 5.5.3 Parâmetros da linha de comando

O ESET SysInspector suporta a geração de relatórios a partir da linha de comando utilizando estes parâmetros:

| | |
|---|---|
| **/gen** | gerar um log diretamente a partir da linha de comando sem executar a GUI |
| **/privacy** | gerar um log excluindo informações confidenciais |
| **/zip** | armazenar o log resultante diretamente no disco em um arquivo compactado |
| **/silent** | ocultar a exibição da barra de progresso da geração de logs |
| **/help, /?** | exibir informações sobre os parâmetros da linha de comando |

**Exemplos**

Para carregar um log específico diretamente no navegador, use: SysInspector.exe "c:\clientlog.xml"
Para gerar um log em um local atual, use: SysInspector.exe /gen
Para gerar um log em uma pasta específica, use: SysInspector.exe /gen="c:\folder\"
Para gerar um log em um arquivo/local específico, use: SysInspector.exe /gen="c:\folder\mynewlog.xml"
Para gerar um log que exclua informações confidenciais diretamente em um arquivo compactado, use: SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip
Para comparar dois logs, use: SysInspector.exe "current.xml" "original.xml"

**OBSERVAÇÃO:** Se o nome do arquivo/pasta contiver uma lacuna, ele deve ser colocado entre aspas.

### 5.5.4 Script de serviços

O script de serviços é uma ferramenta que fornece ajuda aos clientes que utilizam o ESET SysInspector removendo facilmente os objetos indesejados do sistema.

O script de serviços permite que o usuário exporte o relatório completo do ESET SysInspector ou suas partes selecionadas. Após a exportação, você pode marcar os objetos não desejados para exclusão. Em seguida, você pode executar o log modificado para excluir os objetos marcados.

O script de serviços é adequado para usuários avançados com experiência anterior em diagnóstico de problemas do sistema. As modificações não qualificadas podem levar a danos no sistema operacional.

**Exemplo**

Se você suspeita que o seu computador está infectado por um vírus que não é detectado pelo seu programa antivírus, siga estas instruções passo a passo:

- Execute o ESET SysInspector para gerar um novo instantâneo do sistema.
- Selecione o primeiro item na seção à esquerda (na estrutura em árvore), pressione Ctrl e selecione o último item para marcar todos os itens.
- Clique com o botão direito do mouse nos objetos selecionados e selecione a opção do menu de contexto **Exportar as seções selecionadas para script de serviços**.
- Os objetos selecionados serão exportados para um novo log.
- Esta é a etapa mais crucial de todo o procedimento: abra o novo log e altere o atributo - para + em todos os objetos que desejar remover. Verifique se não marcou arquivos/objetos do sistema operacional importantes.
- Abra o ESET SysInspector, clique em **Arquivo** > **Executar script de serviços** e insira o caminho para o script.
- Clique em **OK** para executar o script.

### 5.5.4.1 Geração do script de serviços

Para gerar um script, clique com o botão direito em um item na árvore de menus (no painel esquerdo) na janela principal do ESET SysInspector . No menu de contexto, selecione a opção **Exportar todas as seções para script de serviços** ou a opção **Exportar as seções selecionadas para script de serviços**.

**OBSERVAÇÃO:** Não é possível exportar o script de serviços quando dois logs estiverem sendo comparados.

### 5.5.4.2 Estrutura do script de serviços

Na primeira linha do cabeçalho do script, pode encontrar informações sobre a versão do Mecanismo (ev), versão da GUI (gv) e a versão do log (lv). É possível usar esses dados para rastrear possíveis alterações no arquivo .xml que gera o script e evitar inconsistências durante a execução. Esta parte do script não deve ser alterada.

O restante do arquivo é dividido em seções nas quais os itens podem ser editados (refere-se àqueles que serão processadas pelo script). Marque os itens para processamento substituindo o caractere "-" em frente a um item pelo caractere "+". As seções no script são separadas das outras por uma linha vazia. Cada seção tem um número e um título.

**01) Processos em execução**

Esta seção contém uma lista de todos os processos em execução no sistema. Cada processo é identificado por seu caminho UNC e, subsequentemente, por seu código hash CRC16 em asteriscos (*).

Exemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Neste exemplo, o processo, module32.exe, foi selecionado (marcado por um caractere "+"); o processo será encerrado com a execução do script.

**02) Módulos carregados**

Essa seção lista os módulos do sistema em uso no momento.

Exemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Neste exemplo, o módulo khbekhb.dll foi marcado por um caractere "+". Quando o script for executado, ele reconhecerá os processos que usam esse módulo específico e os encerrará.

**03) Conexões TCP**

Esta seção contém informações sobre as conexões TCP existentes.

Exemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nas conexões TCP marcadas e interromperá o soquete, liberando recursos do sistema.

**04) Pontos de extremidade UDP**

Esta seção contém informações sobre os pontos de extremidade UDP existentes.

Exemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Quando o script for executado, ele isolará o proprietário do soquete nos pontos de extremidade UDP marcados e interromperá o soquete.

### 05) Entradas do servidor DNS

Esta seção contém informações sobre a configuração atual do servidor DNS.

Exemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

As entradas marcadas do servidor DNS serão removidas quando você executar o script.

### 06) Entradas importantes do registro

Esta seção contém informações sobre as entradas importantes do registro.

Exemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

As entradas marcadas serão excluídas, reduzidas ao valor de 0 byte ou redefinidas aos valores padrão com a execução do script. A ação a ser aplicada a uma entrada específica depende da categoria da entrada e do valor da chave no registro específico.

### 07) Serviços

Esta seção lista os serviços registrados no sistema.

Exemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Os serviços marcados e seus serviços dependentes serão interrompidos e desinstalados quando o script for executado.

### 08) Drivers

Esta seção lista os drivers instalados.

Exemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Ao executar o script, os drivers selecionados serão parados. Observe que alguns drivers não permitirão serem parados.

**09) Arquivos críticos**

Esta seção contém informações sobre os arquivos que são críticos para o funcionamento correto do sistema operacional.

Exemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Os itens selecionados serão excluídos ou redefinidos aos valores padrão originais.

### 5.5.4.3 Execução de scripts de serviços

Marque todos os itens desejados, depois salve e feche o script. Execute o script editado diretamente na janela principal do ESET SysInspector selecionando a opção **Executar script de serviços** no menu Arquivo. Ao abrir um script, o programa solicitará que você responda à seguinte mensagem: **Tem certeza de que deseja executar o script de serviços "%Scriptname%"?** Após confirmar a seleção, outro aviso pode ser exibido, informando que o script de serviços que você está tentando executar não foi assinado. Clique em **Executar** para iniciar o script.

Uma janela de diálogo confirmará que o script foi executado com êxito.

Se o script puder ser apenas parcialmente processado, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços foi executado parcialmente. Deseja exibir o relatório de erros?** Selecione **Sim** para exibir um relatório de erro complexo que lista as operações que não foram executadas.

Se o script não for reconhecido, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços selecionado não está assinado. A execução de scripts não assinados e desconhecidos pode danificar seriamente os dados do computador. Tem certeza de que deseja executar o script e realizar as ações?** Isso pode ser causado por inconsistências no script (cabeçalho danificado, título da seção corrompido, ausência de linha vazia entre as seções, etc.). É possível reabrir o arquivo de script e corrigir os erros no script ou criar um novo script de serviços.

## 5.5.5 FAQ

**O ESET SysInspector requer privilégios de administrador para ser executado?**

Enquanto o ESET SysInspector não requer privilégios de administrador para ser executado, algumas das informações que ele coleta apenas podem ser acessadas a partir de uma conta do administrador. A execução desse programa como Usuário padrão ou Usuário restrito fará com que ele colete menos informações sobre o seu ambiente operacional.

**O ESET SysInspector cria um arquivo de log?**

O ESET SysInspector pode criar um arquivo de log da configuração do computador. Para salvar um arquivo de log, selecione **Arquivo** > **Salvar relatório** no menu principal. Os arquivos de log são salvos em formato XML. Por padrão, os arquivos são salvos no diretório %USERPROFILE%\My Documents\, com uma convenção de nomenclatura de arquivos de "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". Você pode alterar o local e o nome do arquivo de log

para outro nome ou local antes de salvá-lo, se preferir.

**Como visualizar o arquivo de log do ESET SysInspector?**

Para visualizar um arquivo de log criado pelo ESET SysInspector, execute o programa e selecione **Arquivo** > **Abrir relatório** no menu principal. Você também pode arrastar e soltar arquivos de log no aplicativo ESET SysInspector. Se você precisar visualizar os arquivos de log do ESET SysInspector com frequência, recomendamos a criação de um atalho para o arquivo SYSINSPECTOR.EXE na área de trabalho; é possível arrastar e soltar os arquivos de log para visualização. Por motivo de segurança, o Windows Vista/7 pode não permitir operações de arrastar e soltar entre janelas que tenham permissões de segurança diferentes.

**Há uma especificação disponível para o formato do arquivo de log? E um SDK?**

Atualmente, não há uma especificação para o arquivo de log nem um SDK disponíveis, uma vez que o programa ainda está em desenvolvimento. Após o lançamento do programa, podemos fornecê-los com base nas informações fornecidas pelos clientes e sob demanda.

**Como o ESET SysInspector avalia o risco representado por um objeto específico?**

Na maioria dos casos, o ESET SysInspector atribui níveis de risco a objetos (arquivos, processos, chaves de registro e assim por diante), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 - Aceitável (verde) a 9 – Perigoso (vermelho). No painel de navegação esquerdo, as seções são coloridas com base no nível de risco mais alto de um objeto dentro delas.

**Um nível de risco "6 - Desconhecido (vermelho)" significa que um objeto é perigoso?**

As avaliações do ESET SysInspector não garantem que um objeto seja malicioso; essa determinação deve ser feita por um especialista em segurança. O ESET SysInspector é destinado a fornecer uma avaliação rápida para especialistas em segurança, para que eles saibam quais objetos em um sistema eles poderão querer examinar quanto a comportamento incomum.

**Por que o ESET SysInspector conecta-se à Internet quando está em execução?**

Como muitos aplicativos, o ESET SysInspector é assinado com um "certificado" de assinatura digital para ajudar a garantir que o software foi publicado pela ESET e que não foi alterado. Para verificar o certificado, o sistema operacional entra em contato com uma autoridade de certificação para verificar a identidade do editor do software. Esse é um comportamento normal para todos os programas assinados digitalmente no Microsoft Windows.

**O que é a tecnologia Anti-Stealth?**

A tecnologia Anti-Stealth proporciona a detecção efetiva de rootkits.

Se o sistema for atacado por um código malicioso que se comporte como um rootkit, o usuário poderá ser exposto à perda ou ao roubo de dados. Sem uma ferramenta especial anti-rootkit, é quase impossível detectar rootkits.

**Por que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente ao mesmo tempo?**

Ao tentar identificar a assinatura digital de um arquivo executável, o ESET SysInspector primeiro verifica se há uma assinatura digital incorporada no arquivo. Se uma assinatura digital for encontrada, o arquivo será validado usando essa informação. Se a assinatura digital não for encontrada, o ESI iniciará a procura do arquivo CAT (Security Catalog - %systemroot%\system32\catroot) correspondente que contenha informações sobre o arquivo executável processado. Caso o arquivo CAT relevante seja encontrado, sua assinatura digital será aplicada no processo de validação do executável.

É por isso que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente.

Exemplo:

O Windows 2000 inclui o aplicativo HyperTerminal, localizado em C:\Arquivos de Programas\Windows NT. O arquivo executável principal do aplicativo não é assinado digitalmente, mas o ESET SysInspector o marca como um arquivo assinado pela Microsoft. O motivo disso é a referência em C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat que aponta para C:\Arquivos de Programas\Windows NT\hypertrm.exe (o executável principal do aplicativo HyperTerminal) e o sp4.cat é digitalmente assinado pela Microsoft.

### 5.5.6 ESET SysInspector como parte do ESET Endpoint Security

Para abrir a seção do ESET SysInspector no ESET Endpoint Security, clique em **Ferramentas** > **ESET SysInspector**. O sistema de gerenciamento na janela do ESET SysInspector é semelhante ao sistema dos relatórios de rastreamento do computador ou das tarefas agendadas. Todas as operações com instantâneos: criar, visualizar, comparar, remover e exportar podem ser acessadas com um ou dois cliques.

A janela do ESET SysInspector contém informações básicas sobre os snapshots criados, como a hora da criação, breve comentário, nome do usuário que criou o snapshot e o status do snapshot.

Para comparar, criar ou excluir instantâneos, utilize os botões correspondentes localizados abaixo da lista de instantâneos na janela do ESET SysInspector . Essas opções também estão disponíveis no menu de contexto. Para exibir o instantâneo do sistema selecionado, utilize a opção do menu de contexto **Mostrar**. Para exportar o instantâneo selecionado para um arquivo, clique com o botão direito e selecione **Exportar...**

Abaixo, veja uma descrição detalhada das opções disponíveis:

- **Comparar** - Permite comparar dois logs existentes. Ela é adequada se você desejar controlar alterações entre o log atual e um log anterior. Para que essa opção entre em vigor, é necessário selecionar dois instantâneos a serem comparados.
- **Criar...** - Cria um novo registro. Antes disso, é preciso inserir um breve comentário sobre o registro. Para saber mais sobre o progresso de criação de instantâneos (do instantâneo gerado no momento), consulte a coluna **Status**. Todos os instantâneos concluídos são marcados com o status **Criado**.
- **Excluir/Excluir tudo** - Remove as entradas da lista.
- **Exportar...** – Salva a entrada selecionada em um arquivo XML (também em uma versão compactada).

## 5.6 ESET SysRescue

O ESET SysRescue é um utilitário que permite a criação de um disco de inicialização contendo uma das soluções ESET Security, podendo ser o ESET NOD32 Antivirus, o ESET Smart Security ou até mesmo algum dos produtos orientados ao servidor. A principal vantagem do ESET SysRescue é o fato de a solução ESET Security ser executada de maneira independente do sistema operacional host, possuindo ao mesmo tempo um acesso direto ao disco e a todo o sistema de arquivos. Isso permite remover infiltrações que normalmente não poderiam ser excluídas, por exemplo, quando o sistema operacional está em execução, etc.

### 5.6.1 Requisitos mínimos

O ESET SysRescue funciona no Microsoft Windows Preinstallation Environment (Windows PE) versão 2.x, que é baseado no Windows Vista.

O Windows PE faz parte do pacote gratuito Windows Automated Installation Kit (Windows AIK), portanto o Windows AIK deve ser instalado antes da criação do ESET SysRescue (http://go.eset.eu/AIK). Devido ao suporte da versão de 32 bits do Windows PE, é necessário usar o pacote de instalação de 32 bits da solução ESET Security ao criar o ESET SysRescue em sistemas de 64 bits. O ESET SysRescue é compatível com o Windows AIK 1.1 e versões posteriores.

**OBSERVAÇÃO:** Como o Windows AIK é maior que 1 GB, uma conexão com a Internet de alta velocidade é necessária para um download perfeito.

O ESET SysRescue está disponível nas soluções ESET Security 4.0 e versões posteriores.

**Sistemas operacionais compatíveis**

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 com KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 com KB926044
- Windows XP Service Pack 3

### 5.6.2 Como criar o CD de restauração

Para iniciar o assistente do ESET SysRescue, clique em **Iniciar** > **Programas** > **ESET** > **ESET Endpoint Security** > **ESET SysRescue**.

Primeiro, o assistente verifica a presença do Windows AIK e de um dispositivo adequado para a criação da mídia de inicialização. Se o Windows AIK não estiver instalado no computador (ou estiver corrompido ou instalado incorretamente), o assistente dará a opção de instalá-lo ou de inserir o caminho para a pasta do Windows AIK (http://go.eset.eu/AIK).

**OBSERVAÇÃO:** Como o Windows AIK é maior que 1 GB, uma conexão com a Internet de alta velocidade é necessária para um download perfeito.

Na próxima etapa, selecione a mídia de destino em que o ESET SysRescue estará localizado.

### 5.6.3 Seleção de alvos

Além de CD/DVD/USB, você pode escolher salvar o ESET SysRescue em um arquivo ISO. Posteriormente, é possível gravar a imagem ISO em CD/DVD ou utilizá-la de alguma outra maneira (por exemplo, no ambiente virtual, como VMWare ou VirtualBox).

Se você selecionar USB como a mídia-alvo, a reinicialização pode não funcionar em determinados computadores. Algumas versões de BIOS podem relatar problemas com o BIOS - comunicação com o gerenciador de inicialização (por exemplo, no Windows Vista), e a inicialização é encerrada com a seguinte mensagem de erro:

```
arquivo: \boot\bcd
status: 0xc000000e
informações: an error occurred while attemping to read the boot configuration data (ocorreu um erro ao tenta
```

Se você encontrar essa mensagem, recomendamos que selecione o CD, em vez da mídia USB.

### 5.6.4 Configurações

Antes de iniciar a criação do ESET SysRescue, o assistente de instalação exibe os parâmetros de compilação na última etapa do assistente do ESET SysRescue. Para modificá-los, clique no botão **Alterar...**. As opções disponíveis incluem:

- Pastas
- Antivírus ESET
- Avançado
- Protoc. Internet
- Dispositivo USB inicializável (quando o dispositivo USB de destino é selecionado)
- Gravação (quando a unidade de CD/DVD de destino é selecionada)

O botão **Criar** estará inativo se nenhum pacote de instalação MSI for especificado ou se nenhuma solução ESET Security estiver instalada no computador. Para selecionar um pacote de instalação, clique no botão **Alterar** e vá para a guia **Antivírus ESET**. Além disso, se você não preencher o nome do usuário e a senha (**Alterar** > **Antivírus ESET**), o botão **Criar** estará acinzentado.

#### 5.6.4.1 Pastas

A **Pasta temporária** é um diretório de trabalho para arquivos exigidos durante a compilação do ESET SysRescue.

**Pasta ISO** é uma pasta, em que o arquivo ISO resultante é salvo após a conclusão da compilação.

A lista nessa guia mostra todas as unidades de rede locais e mapeadas, junto com o espaço livre disponível. Se algumas das pastas estiverem localizadas em uma unidade com espaço livre insuficiente, recomendamos que você selecione outra unidade com mais espaço livre disponível. Caso contrário, a compilação pode terminar prematuramente devido a espaço livre em disco insuficiente.

**Aplicativos externos** - Permite especificar os programas adicionais que serão executados ou instalados após a inicialização a partir de uma mídia do ESET SysRescue.

**Incluir aplicativos externos** - Permite adicionar programas externos à compilação do ESET SysRescue.

**Pasta selecionada** - Pasta na qual os programas a serem adicionados ao disco do ESET SysRescue estão localizados.

#### 5.6.4.2 Antivírus ESET

Para criar o CD do ESET SysRescue, é possível selecionar duas fontes de arquivos da ESET para serem utilizadas pelo compilador.

**Pasta do ESS/EAV** - Arquivos já contidos na pasta na qual a solução ESET Security está instalada no computador.

**Arquivo MSI** - São usados os arquivos contidos no instalador do MSI.

Em seguida, é possível atualizar a localização dos arquivos (.nup). Normalmente, a opção padrão **Pasta do ESS/EAV/ Arquivo MSI** deve ser definida. Em alguns casos, uma **Pasta de atualização** personalizada pode ser definida, por exemplo, para usar uma versão mais antiga ou mais recente de um banco de dados de assinatura de vírus.

É possível utilizar uma das seguintes fontes de nome de usuário e senha:

**ESS/EAV instalado** - O nome de usuário e a senha são copiados da solução ESET Security instalada no momento.

**Do usuário** - O nome de usuário e a senha digitados nas caixas de texto correspondentes serão utilizados.

**OBSERVAÇÃO:** A solução ESET Security no CD do ESET SysRescue é atualizada a partir da Internet ou da solução ESET Security instalada no computador em que o CD do ESET SysRescue for executado.

#### 5.6.4.3 Configurações avançadas

A guia **Avançado** permite otimizar o CD do ESET SysRescue de acordo com o tamanho da memória do computador. Selecione **576 MB ou mais** para gravar o conteúdo do CD na memória operacional (RAM). Se você selecionar **menos de 576 MB**, o CD de recuperação será permanentemente acessado quando o WinPE estiver em execução.

Na seção **Drivers externos**, é possível inserir drivers para o seu hardware específico (geralmente o adaptador de rede). Embora o WinPE seja baseado no Windows Vista SP1, que suporta uma larga escala de hardware, algumas vezes o hardware não é reconhecido. Isso requer que o driver seja adicionado manualmente. Há duas maneiras de inserir o driver em uma compilação do ESET SysRescue - manualmente (botão **Adicionar**) e automaticamente (botão **Pesquisa auto**). No caso de inclusão manual, é preciso selecionar o caminho para o arquivo .inf correspondente (o arquivo *.sys aplicável também deve estar presente nessa pasta). No caso de inserção automática, o driver é encontrado automaticamente no sistema operacional do computador específico. Recomendamos que use a inclusão automática apenas se o ESET SysRescue for usado em um computador com o mesmo adaptador de rede usado no computador em que o CD ESET SysRescue foi criado. Durante a criação, o driver do ESET SysRescue é inserido na compilação para que você não precise procurá-lo depois.

#### 5.6.4.4 Protoc. Internet

Essa seção permite configurar informações básicas de rede e definir as conexões predefinidas após o ESET SysRescue.

Selecione **Endereço IP privado autom.** para obter o endereço IP automaticamente a partir do servidor DHCP (Dynamic Host Configuration Protocol, protocolo de configuração dinâmica de endereços de rede).

Se preferir, a conexão de rede pode usar um endereço IP especificado manualmente (também conhecido como endereço IP estático). Selecione **Personalizar** para definir as configurações adequadas para o endereço IP. Ao definir essa opção, é preciso especificar um **Endereço IP** e, para a LAN e as conexões de Internet de alta velocidade, uma **Máscara de sub-rede**. Em **Servidor DNS preferencial** e **Servidor DNS alternativo**, digite os endereços principal e secundário do servidor DNS.

#### 5.6.4.5 Dispositivo USB inicializável

Se você selecionou um dispositivo USB como mídia-alvo, é possível selecionar um dos dispositivos USB disponíveis na guia **Dispositivo USB inicializável** (caso haja mais dispositivos USB).

Selecione o **Dispositivo** de destino apropriado onde o ESET SysRescue será instalado.

**Aviso**: O dispositivo USB selecionado será formatado durante a criação do ESET SysRescue. Todos os dados no dispositivo serão excluídos.

Se você optar por uma **Formatação rápida**, a formatação removerá todos os arquivos da partição, mas não rastreará o disco em busca de setores corrompidos. Use essa opção se o dispositivo USB tiver sido formatado anteriormente e você tiver certeza de que ele não está danificado.

#### 5.6.4.6 Gravar

Se você selecionou CD/DVD como sua mídia-alvo, é possível especificar parâmetros de gravação adicionais na guia **Gravar**.

**Excluir arquivo ISO** - Marque essa opção para excluir o arquivo ISO temporário após o CD do ESET SysRescue ser criado.

**Exclusão ativada** - Permite selecionar o apagamento rápido e concluí-lo.

**Dispositivo de gravação** - Selecione a unidade a ser utilizada para gravação.

**Aviso:** Essa é a opção padrão. Se um CD/DVD regravável for usado, todos os dados contidos no CD/DVD serão apagados.

A seção Mídia contém informações sobre a mídia no seu dispositivo de CD/DVD.

**Velocidade de gravação** - Selecione a velocidade desejada no menu suspenso. Os recursos do seu dispositivo de gravação e o tipo de CD/DVD utilizado devem ser considerados ao selecionar a velocidade da gravação.

### 5.6.5 Trabalhar com o ESET SysRescue

Para o CD/DVD/USB de restauração funcionar de forma eficiente, é necessário que o computador seja inicializado a partir da mídia de inicialização do ESET SysRescue. A prioridade de inicialização pode ser modificada no BIOS. Como alternativa, você pode usar o menu de inicialização durante a inicialização do computador, geralmente utilizando uma das teclas: F9 a F12, dependendo da versão da placa-mãe/do BIOS.

Após a inicialização da mídia de inicialização, a solução ESET Security será iniciada. Como o ESET SysRescue é utilizado apenas em situações específicas, alguns módulos de proteção e recursos do programa presentes na versão padrão da solução ESET Security não são necessários; a lista é limitada ao **Rastreamento do computador**, à opção **Atualizar**, e algumas seções da **Configuração**. A capacidade de atualizar o banco de dados de assinaturas de vírus é o recurso mais importante do ESET SysRescue. Recomendamos que você atualize o programa antes de iniciar um rastreamento do computador.

#### 5.6.5.1 Utilização do ESET SysRescue

Suponha que os computadores na rede tenham sido infectados por um vírus que modifica os arquivos executáveis (. exe). A solução ESET Security consegue limpar todos os arquivos infectados, exceto o explorer.exe, que não pode ser limpo, mesmo no modo de segurança. Isso ocorre porque o explorer.exe, como um dos processos essenciais do Windows, também é iniciado no modo de segurança. A solução ESET Security não poderia realizar ações com o arquivo e ele permaneceria infectado.

Nesse tipo de cenário, seria possível usar o ESET SysRescue para solucionar o problema. O ESET SysRescue não requer componentes do sistema operacional host, portanto ele pode processar (limpar, excluir) qualquer arquivo no disco.

# 6. Glossário

## 6.1 Tipos de infiltrações

Uma infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

### 6.1.1 Vírus

Um vírus de computador é uma parte de um código malicioso que é pré-anexado ou anexado a arquivos existentes no computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro. Quanto ao termo "vírus", ele é frequentemente usado de maneira incorreta para significar qualquer tipo de ameaça. Essa utilização está gradualmente sendo superada e substituída por um termo mais preciso "malware" (software malicioso).

Os vírus de computador atacam principalmente os arquivos e documentos executáveis. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o código malicioso é chamado e executado antes da execução do aplicativo original. Um vírus pode infectar qualquer arquivo que tenha permissão de gravação dada pelo usuário.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositadamente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

Se o computador estiver infectado com um vírus e a limpeza não for possível, envie-o para o laboratório da ESET para análise. Em certos casos os arquivos infectados podem ser modificados a ponto de uma limpeza não ser possível e os arquivos precisarem ser substituídos por uma cópia limpa.

### 6.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se propagar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms propagam-se para os endereços de email da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais viáveis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de horas ou mesmo minutos após sua liberação. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversas inconveniências: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

### 6.1.3 Cavalos de Troia

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de ameaças que tentam se apresentar como programas úteis, enganando assim os usuários para executá-los.

Dado que Cavalos de Troia são uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- **Downloader** - Programas maliciosos com a capacidade de fazer o download de outras ameaças da Internet.
- **Dropper** - Programas maliciosos com a capacidade para instalar outros tipos de malware em computadores comprometidos.
- **Backdoor** - Programas maliciosos que se comunicam com atacantes remotos, permitindo que eles acessem o computador e assumam o seu controle.
- **Keylogger** - (keystroke logger) - Um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- **Dialer** - Programas maliciosos projetados para se conectar aos números premium-rate em vez do provedor de serviços de Internet do usuário. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modens discados que não são mais usados regularmente.

Se um arquivo em seu computador for detectado como um cavalo de troia, é aconselhável excluí-lo, uma vez que ele contém códigos maliciosos.

### 6.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows. Por essa razão, é quase impossível detectá-los usando as técnicas comuns.

Há dois níveis de detecção para impedir rootkits:

1. Quando eles tentam acessar um sistema. Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).
2. Quando eles estão ocultos para os testes usuais. Os usuários do ESET Endpoint Security têm a vantagem da tecnologia Anti-Stealth, que também é capaz de detectar e eliminar os rootkits ativos.

### 6.1.5 Adware

Adware é abreviação de "advertising-supported software" (software suportado por propaganda). Os programas exibindo material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a homepage do mesmo. O adware é frequentemente vinculado a programas freeware, permitindo que seus criadores cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso - os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware pode também realizar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa da instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware.

Alguns programas não serão instalados sem o adware ou as suas funcionalidades serão limitadas. Isso significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar. Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há grande possibilidade de que contenha códigos maliciosos.

### 6.1.6 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de email da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINs, números de contas bancárias, etc. O Spyware frequentemente é vinculado a versões gratuitas de um programa pelo seu autor a fim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável excluí-lo, uma vez que há grande probabilidade de ele conter códigos maliciosos.

### 6.1.7 Aplicativos potencialmente inseguros

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. O ESET Endpoint Security fornece a opção de detectar tais ameaças.

**Aplicativos potencialmente inseguros** é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo não seguro em potencial presente e sendo executado em seu computador (e que você não instalou), favor consultar o seu administrador de rede ou remover o aplicativo.

### 6.1.8 Aplicativos potencialmente indesejados

Os **Aplicativos potencialmente indesejados** (PUAs) não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são:

- Novas janelas que você não via anteriormente (pop-ups, ads).
- Ativação e execução de processos ocultos.
- Uso aumentado de recursos do sistema.
- Alterações nos resultados de pesquisa.
- O aplicativo comunica-se com servidores remotos.

## 6.2 Tipos de ataques remotos

Há muitas técnicas especiais que permitem que os agressores comprometam os sistemas remotos. Elas são divididas em diversas categorias.

### 6.2.1 Ataques DoS

DoS, ou Denial of Service (negação de serviço), é a tentativa de impedir que o computador ou a rede sejam acessados por seus usuários. A comunicação entre os usuários afetados é obstruída e não pode mais continuar de modo funcional. Os computadores expostos aos ataques DoS geralmente precisam ser reinicializados para que voltem a funcionar adequadamente.

Na maioria dos casos, os alvos são servidores web e o objetivo é torná-los indisponíveis aos usuários por um determinado período de tempo.

### 6.2.2 Envenenamento de DNS

Através do envenenamento de DNS (Domain Name Server), os hackers podem levar o servidor DNS de qualquer computador a acreditar que os dados falsos que eles forneceram são legítimos e autênticos. As informações falsas são armazenadas em cache por um determinado período de tempo, permitindo que os agressores reescrevam as respostas do DNS dos endereços IP. Como resultado, os usuários que tentarem acessar os websites da Internet farão o download de vírus ou worms no lugar do seu conteúdo original.

### 6.2.3 Ataques de worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. Os worms da rede exploram as vulnerabilidades de segurança dos diversos aplicativos. Devido à disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de algumas horas após sua liberação. Em alguns casos, até mesmo em minutos.

A maioria dos ataques dos worms (Sasser, SqlSlammer) podem ser evitados usando-se as configurações de segurança padrão do firewall, ou bloqueando as portas não usadas e desprotegidas. Também é fundamental manter o sistema operacional atualizado com os patches de segurança mais recentes.

### 6.2.4 Rastreamento de portas

O rastreamento de portas é usado para determinar se há portas abertas no computador em um host de rede. Um rastreador de porta é um software desenvolvido para encontrar tais portas.

Uma porta de computador é um ponto virtual que lida com os dados de entrada e saída - ação crucial do ponto de vista da segurança. Em uma rede grande, as informações reunidas pelos rastreadores de porta podem ajudar a identificar as vulnerabilidades em potencial. Tal uso é legítimo.

O rastreamento de porta é frequentemente usado pelos hackers na tentativa de comprometer a segurança. Seu primeiro passo é enviar pacotes para cada porta. Dependendo do tipo de resposta, é possível determinar quais portas estão em uso. O rastreamento por si só não causa danos, mas esteja ciente de que essa atividade pode revelar as vulnerabilidades em potencial e permitir que os agressores assumam o controle remoto dos computadores.

Os administradores de rede são aconselhados a bloquear todas as portas não usadas e proteger as que estão em uso contra o acesso não autorizado.

### 6.2.5 Dessincronização TCP

A dessincronização TCP é uma técnica usada nos ataques do TCP Hijacking. Ela é acionada por um processo no qual o número sequencial dos pacotes recebidos difere do número sequencial esperado. Os pacotes com um número sequencial inesperado são dispensados (ou salvos no armazenamento do buffer, se estiverem presentes na janela de comunicação atual).

Na dessincronização, os dois pontos finais da comunicação dispensam os pacotes recebidos; esse é o ponto onde os agressores remotos são capazes de se infiltrar e fornecer pacotes com um número sequencial correto. Os agressores podem até manipular ou modificar a comunicação.

Os ataques TCP Hijacking têm por objetivo interromper as comunicações servidor-cliente ou peer-to-peer. Muitos ataques podem ser evitados usando autenticação para cada segmento TCP. Também é aconselhável usar as configurações recomendadas para os seus dispositivos de rede.

### 6.2.6 Relé SMB

O Relé SMB e o Relé SMB 2 são programas especiais capazes de executar um ataque contra computadores remotos. Os programas se aproveitam do protocolo de compartilhamento do arquivo Server Message Block que é embutido no NetBios. Se um usuário compartilhar qualquer pasta ou diretório dentro da LAN, provavelmente ele utilizará esse protocolo de compartilhamento de arquivo.

Dentro da comunicação de rede local, as criptografias da senha são alteradas.

O Relé SMB recebe uma conexão nas portas UDP 139 e 445, detecta os pacotes trocados pelo cliente e o servidor e os modifica. Após conectar e autenticar, o cliente é desconectado. O Relé SMB cria um novo endereço IP virtual. O novo endereço pode ser acessado usando o comando "net use \\192.168.1.1". O endereço pode então ser usado por qualquer uma das funções de rede do Windows. O Relé SMB detecta a comunicação do protocolo SMB, exceto para negociação e autenticação. Os agressores remotos podem usar o endereço IP enquanto o computador cliente estiver conectado.

O Relé SMB 2 funciona com o mesmo princípio do Relé SMB, exceto que ele usa os nomes do NetBios no lugar dos endereços IP. Os dois executam ataques "man-in-the-middle". Esses ataques permitem que os agressores remotos leiam, insiram e modifiquem as mensagens trocadas entre dois pontos finais de comunicação sem serem notados. Os computadores expostos a tais ataques frequentemente param de responder ou reiniciam inesperadamente.

Para evitar ataques, recomendamos que você use senhas ou chaves de autenticação.

### 6.2.7 Ataques ICMP

O ICMP (Protocolo de Controle de Mensagens da Internet) é um protocolo de Internet popular e amplamente utilizado. Ele é utilizado primeiramente por computadores em rede para enviar várias mensagens de erro.

Os atacantes remotos tentam explorar a fraqueza do protocolo ICMP. O protocolo ICMP é destinado para a comunicação unidirecional que não requer qualquer autenticação. Isso permite que os atacantes remotos disparem ataques chamados de DoS (negação de serviço) ou ataques que dão acesso a pessoas não autorizadas aos pacotes de entrada e de saída.

Exemplos típicos de um ataque ICMP são ping flood, flood de ICMP_ECHO e ataques de smurfs. Os computadores expostos ao ataque ICMP são significativamente mais lentos (isso se aplica a todos os aplicativos que utilizam a Internet) e têm problemas para conectarem-se à Internet.

## 6.3 Email

Email ou correio eletrônico é uma forma moderna de comunicação e traz muitas vantagens. Flexível, rápido e direto, o email teve um papel crucial na proliferação da Internet no início dos anos 90.

Infelizmente, com seus altos níveis de anonimato, o email e a Internet abrem espaço para atividades ilegais, como, por exemplo, spams. O spam inclui propagandas não solicitadas, hoaxes e proliferação de software malicioso - malware (códigos maliciosos). A inconveniência e o perigo para você são aumentados pelo fato de que os custos de envio são mínimos e os autores de spam têm muitas ferramentas para obter novos endereços de email. Além disso, o volume e a variedade de spams dificultam muito o controle. Quanto mais você utiliza o seu email, maior é a possibilidade de acabar em um banco de dados de mecanismo de spam. Algumas dicas de prevenção:

- Se possível, não publique seu email na Internet
- Forneça seu email apenas a pessoas confiáveis
- Se possível, não use aliases comuns; com aliases mais complicados, a probabilidade de rastreamento é menor
- Não responda a spam que já chegou à sua caixa de entrada
- Tenha cuidado ao preencher formulários da Internet; tenha cuidado especial com opções, como "Sim, desejo receber informações".
- Use emails "especializados" - por exemplo, um para o trabalho, um para comunicação com amigos, etc.
- De vez em quando, altere o seu email
- Utilize uma solução antispam

### 6.3.1 Propagandas

A propaganda na Internet é uma das formas de publicidade que mais cresce. As suas principais vantagens de marketing são o custo mínimo e um alto nível de objetividade. Além disso, as mensagens são enviadas quase que imediatamente. Muitas empresas usam as ferramentas de marketing por email para comunicar de forma eficaz com os seus clientes atuais e prospectivos.

Esse tipo de publicidade é legítimo, desde que você tenha interesse em receber informações comerciais sobre alguns produtos. Mas muitas empresas enviam mensagens comerciais em bloco não solicitadas. Nesses casos, a publicidade por email ultrapassa o limite razoável e se torna spam.

Hoje em dia a quantidade de emails não solicitados é um problema e não demonstra sinais de que vá diminuir. Geralmente, os autores dos emails não solicitados tentam mascarar o spam como mensagens legítimas.

### 6.3.2 Hoaxes

Um hoax é uma informação incorreta que é propagada pela Internet. Normalmente, os hoaxes são enviados por email ou por ferramentas de comunicação, como ICQ e Skype. A própria mensagem é geralmente uma brincadeira ou uma Lenda urbana.

Os hoaxes de vírus de computador tentam gerar FUD (medo, incerteza e dúvida) nos remetentes, levando-os a acreditar que há um "vírus desconhecido" excluindo arquivos e recuperando senhas ou executando alguma outra atividade perigosa em seu sistema.

Alguns hoaxes solicitam aos destinatários que encaminhem mensagens aos seus contatos, perpetuando-os. Há hoaxes de celular, pedidos de ajuda, pessoas oferecendo para enviar-lhe dinheiro do exterior etc. Na maioria dos casos, é impossível identificar a intenção do criador.

Se você receber uma mensagem solicitando que a encaminhe para todos os contatos que você conheça, ela pode ser muito bem um hoax. Há muitos sites especializados na Internet que podem verificar se o email é legítimo ou não. Antes de encaminhar, faça uma pesquisa na Internet sobre a mensagem que você suspeita que seja um hoax.

### 6.3.3 Roubo de identidade

O termo roubo de identidade define uma atividade criminal que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Seu objetivo é obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN, etc.

O acesso geralmente é feito pelo envio de um email passando-se por uma pessoa ou negócio confiável (por ex. instituição financeira, companhia de seguros). O email parecerá muito legítimo e conterá gráficos e conteúdo que podem vir originalmente da fonte pela qual ele está tentando se passar. Você será solicitado a digitar, sob várias pretensões (verificação dos dados, operações financeiras), alguns dos seus dados pessoais - números de contas bancárias ou nomes de usuário e senhas. Todos esses dados, se enviados, podem ser facilmente roubados ou usados de forma indevida.

Bancos, companhias de seguros e outras empresas legítimas nunca solicitarão nomes de usuário e senhas em um email não solicitado.

### 6.3.4 Reconhecimento de fraudes em spam

Geralmente, há alguns indicadores que podem ajudar a identificar spam (emails não solicitados) na sua caixa de correio. Se uma mensagem atender a pelo menos alguns dos critérios a seguir, muito provavelmente é uma mensagem de spam.

- O endereço do remetente não pertence a alguém da sua lista de contatos.
- Você recebe uma oferta de grande soma de dinheiro, mas tem de fornecer primeiro uma pequena soma.
- Você é solicitado a inserir, sob vários pretextos (verificação de dados, operações financeiras), alguns de seus dados pessoais (números de contas bancárias, nomes de usuário e senhas, etc.)
- Está escrito em um idioma estrangeiro.
- Você é solicitado a comprar um produto no qual você não tem interesse. Se decidir comprar de qualquer maneira, verifique se o remetente da mensagem é um fornecedor confiável (consulte o fabricante do produto original).
- Algumas das palavras estão com erros de ortografia em uma tentativa de enganar o seu filtro de spam. Por exemplo, "vaigra" em vez de "viagra", etc.

#### 6.3.4.1 Regras

No contexto das soluções antispam e dos clientes de email, as regras são as ferramentas para manipular as funções do email. Elas são constituídas por duas partes lógicas:

1. Condição (por exemplo, uma mensagem recebida de um determinado endereço)
2. Ação (por exemplo, a exclusão da mensagem, movendo-a para uma pasta especificada)

O número e a combinação de diversas regras com a solução antispam. Essas regras servem como medidas contra spam (email não solicitado). Exemplos típicos:

- 1. Condição: Uma mensagem de email recebida contém algumas palavras geralmente vistas nas mensagens de spam.
  2. Ação: Excluir a mensagem.

- 1. Condição: Uma mensagem de email recebida contém um anexo com a extensão .exe.
  2. Ação: Excluir o anexo e enviar a mensagem para a caixa de correio.

- 1. Condição: Uma mensagem de email recebida chega do seu patrão.
  2. Ação: Mover a mensagem para a pasta "Trabalho".

Recomendamos que você use uma combinação de regras nos programas antispam a fim de facilitar a administração e filtrar os spams com mais eficiência.

#### 6.3.4.2 Lista de permissões

Em geral, uma lista de permissões é uma lista de itens ou pessoas que são aceites, ou para os quais foi concedida permissão de acesso. O termo "lista de permissões de email" define uma lista de contatos de quem o usuário deseja receber mensagens. Tais listas de permissões são baseadas nas palavras-chave para os endereços de email, nomes de domínio ou endereços IP.

Se uma lista de permissões funcionar de "modo exclusivo", então as mensagens de qualquer outro endereço, domínio ou endereço IP não serão recebidas. Se a lista de permissões não for exclusiva, tais mensagens não serão excluídas, mas filtradas de algum modo.

Uma lista de permissões baseia-se no princípio oposto de uma lista de proibições. As listas de permissões são relativamente fáceis de serem mantidas, mais do que as listas de proibições. Recomendamos que você use tanto a Lista de permissões como a Lista de proibições para filtrar os spams com mais eficiência.

#### 6.3.4.3 Lista de proibições

Geralmente, uma lista de proibições é uma lista de itens ou pessoas proibidos ou inaceitáveis. No mundo virtual, é uma técnica que permite aceitar mensagens de todos os usuários não presentes em uma determinada lista.

Há dois tipos de lista de proibições: as criadas pelos usuários em seus aplicativos antispam e as listas de proibições profissionais atualizadas com frequência, criadas por instituições especializadas e que podem ser encontradas na Internet.

O uso dessas listas de proibições é um componente essencial da filtragem antispam bem-sucedida, mas é muito difícil mantê-la, uma vez que novos itens não bloqueados aparecem todos os dias. Recomendamos o uso de uma lista de permissões e uma lista de proibições para filtrar os spams com a maior eficácia.

#### 6.3.4.4 Controle pelo servidor

O controle pelo servidor é uma técnica para identificar os emails de spam em massa com base no número de mensagens recebidas e nas reações dos usuários. Cada mensagem deixa uma "marca" digital única com base no conteúdo da mensagem. O número de ID único não diz nada sobre o conteúdo do email. Duas mensagens idênticas terão marcas idênticas, enquanto mensagens diferentes terão marcas diferentes.

Se uma mensagem for marcada como spam, sua marca será enviada ao servidor. Se o servidor receber mais marcas idênticas (correspondendo a uma determinada mensagem de spam), a marca será armazenada no banco de dados de marcas de spam. Ao rastrear as mensagens recebidas, o programa envia as marcas das mensagens ao servidor. O servidor retorna as informações sobre que marcas correspondem às mensagens já marcadas pelos usuários como spam.